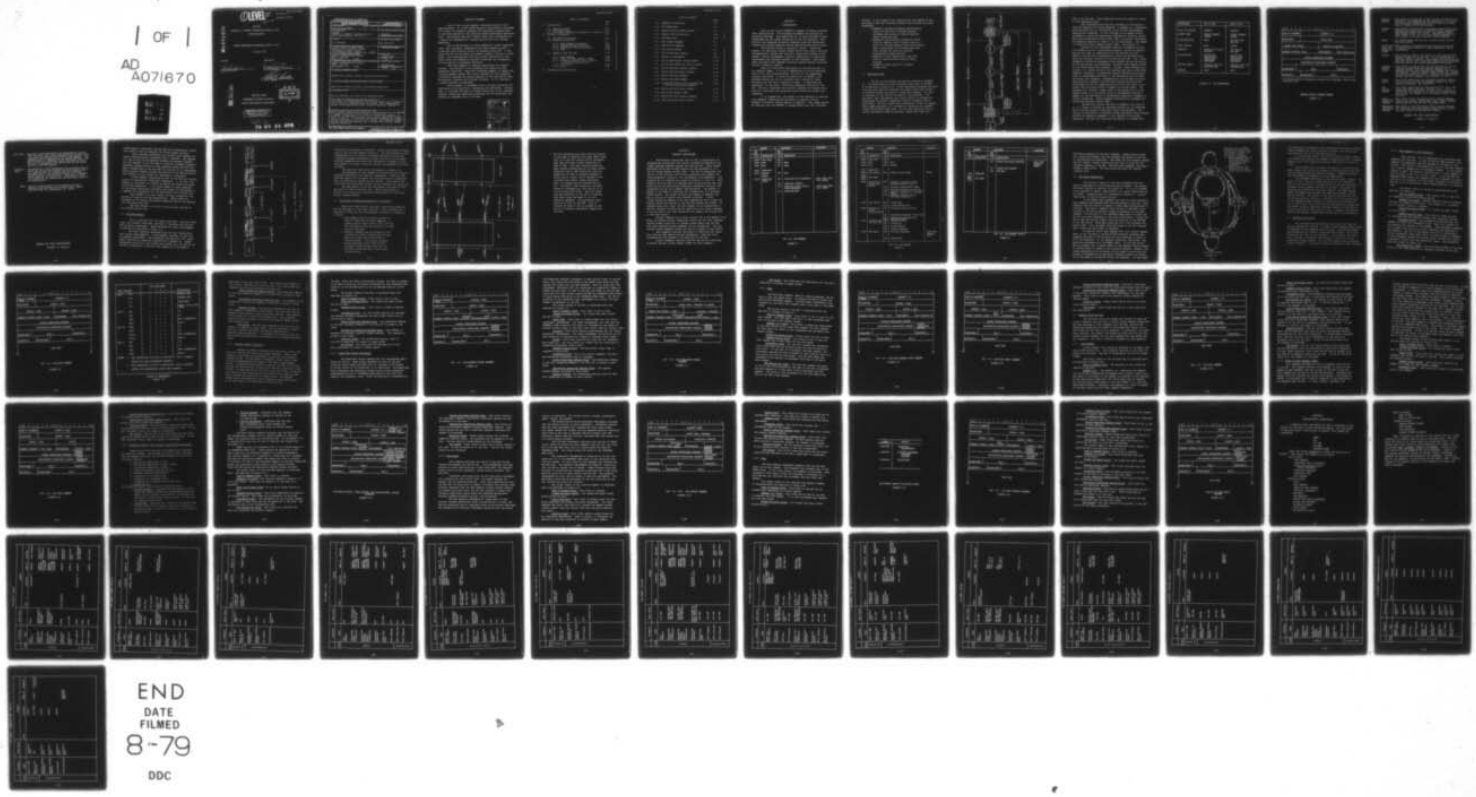
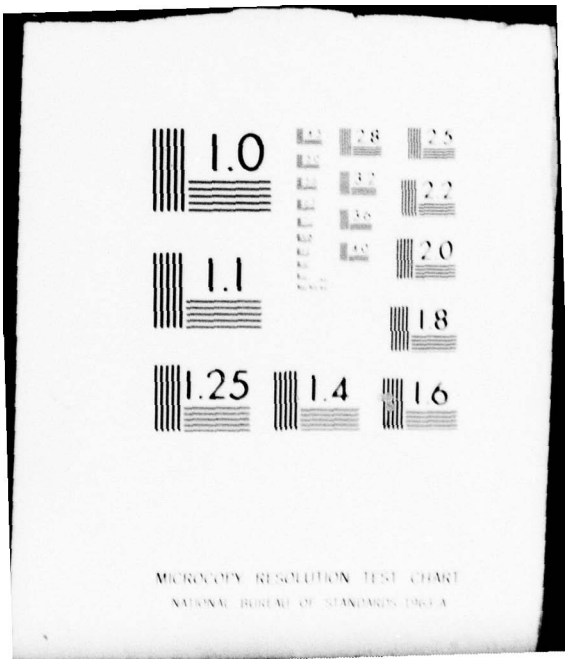
AD-A071 670 WESTERN UNION TELEGRAPH CO MCLEAN VA SYSTEM ENGINEER--ETC F/G 17/2
INITIAL AUTODIN II SEGMENT INTERFACE PROTOCOL (SIP) SPECIFICATI--ETC(U)
MAR 79 V R KULKARNI DCA200-C-0637
UNCLASSIFIED TN-78-07.3 SBIE -AD-E100 245 NL



1 OF 1
AD A071670

END
DATE FILMED
8-79
DDC


1.0
1.1
1.25
1.4
1.6
2.8
2.5
2.2
2.0
1.8
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963-A

LEVEL III

TN 78-07.3

Revised 3/5/79

INITIAL

AUTODIN II SEGMENT INTERFACE PROTOCOL (SIP)

SPECIFICATION

SYSTEM ENGINEERING TECHNICAL NOTE 78-07.3

5 March 1979

Author:

V. R. Kulkarni

Approved:

P. J. Nichols

R. E. Hunter

WESTERN UNION

GOVERNMENT SYSTEMS DIVISION

SYSTEM ENGINEERING DEPARTMENT

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER DCA 200-C-637-P003	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Initial AUTODIN II Segment Interface Protocol (SIP) Specification, TN 78-07.3		5. TYPE OF REPORT & PERIOD COVERED Interim 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) V.R. Kulkarni		8. CONTRACT OR GRANT NUMBER(s) DCA 200-C-637
9. PERFORMING ORGANIZATION NAME AND ADDRESS Western Union Telegraph Company Government Systems Division 7916 Westpark Drive, McLean, VA 22102		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Defense Communications Agency ATTN: Code 450 Washington, D. C. 20305		12. REPORT DATE 5 March 1979 13. NUMBER OF PAGES 68
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office) Defense Communications Agency ATTN: Code 450 Washington, D. C. 20305		15. SECURITY CLASS. (of this report) UNCLASSIFIED 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

Approved for public release; distribution unlimited

18. SUPPLEMENTARY NOTES

Review relevance five years from submission date.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Data Links, Telecommunications, Switching Systems, Data Communications Protocol, Telecommunications Systems, Data Communications System, Telecommunication Links, Network Interface, AUTODIN II

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This document provides the functional specification for the AUTODIN II Segment Interface Protocol (SIP) in the abstract sense. It describes the externally (to the host) visible and mandatory portions of the SIP. It describes the protocol commands and formats, and the prescribed state transition stimuli and responses. This document revises and replaces the 3 October 1978 version, identified as TN-78-07.2.

EXECUTIVE SUMMARY

This is the initial Segment Interface Protocol (SIP) Specification. It is the formal protocol specification developed as a result of extensive redesign and associated changes since it was first defined in the original System Performance Specification. The protocol may still undergo some minor refinements as a result of implementation, system testing and early network operation.

SIP is the protocol by which AUTODIN II access components (TAC, SCCU, and MCCU) communicate with the backbone network. A host may also directly access the backbone using SIP. A host using SIP will be provided pure packet transport service to other hosts. The accountability and flow control functions at this level within the AUTODIN II protocol hierarchy are rudimentary, but the service is extremely efficient.

Each data segment is handled individually and expeditiously. The protocol is not burdened with connection and sequencing functions. Each self contained segment is tagged with a Binary Segment Leader (BSL) which includes all the necessary information required for proper handling to the destination host. The protocol operates with minimal controls. It is, therefore, a simple protocol to implement.

This document is intended to give the Host Subscriber an indication of the protocol's complexity and usefulness. Furthermore, it provides the specific formal definition of SIP commands, formats, states and operating principles for the subscriber who chooses to implement SIP in his host.

TABLE OF CONTENTS

LIST OF FIGURES

SECTION 1

INTRODUCTION

This is the initial AUTODIN II Segment Interface Protocol (SIP) Specification. This Technote documents the protocol as currently designed. This specification is being provided to host subscribers as the formal definition of the SIP protocol. This protocol has undergone extensive redesign since the System Performance and System Technical Design Specifications were written.

The protocol design is basically stable. There may, however, be some minor design changes which could result from the implementation, system test and early operational phases of the system. Design refinements, protocol redefinition or editorial improvements may generate updates to this document. Past experience has shown that computer protocols undergo several revisions during a network's infancy.

This is a functional description of the SIP protocol in its abstract sense. It is not a description of a SIP functional entity (e.g. SIP software module) with all of the associated internal functions. It does not explain how to design a SIP software module nor how to interface such a module to other protocols and the host's operating system. It describes the externally (to the host) visible and mandatory portions of the SIP. Section 2 describes the protocol commands and formats while Section 3 describes the prescribed state transition stimuli and responses.

It is assumed that the reader of this Technote is familiar with computer communications protocols in general and the AUTODIN II protocol layered design in specific. The reader should be familiar with the AUTODIN II system design and user interface

options. If the reader is not familiar with the AUTODIN II system design, then the following documents will provide the proper background:

- o AUTODIN II System Performance Specification (type "A") Nov 1975 as amended through September 1976, plus all approved Specification Change Notices.
- o AUTODIN II System Design (Technical) Specification [Western Union Proposal (Part 5), April 76; plus Refinements and Clarifications, June 76 and August 76; plus Best and Final Offer October 76] plus all approved Specification Change Notices.
- o AUTODIN II Final Design Plan, June 1978, plus all approved Specification Change Notices.
- o AUTODIN II Design Executive Summary, 18 May 1978.

1.1 Overview of SIP

The SIP is the backbone access/exit protocol of AUTODIN II. Its relationship to other protocols that exist in AUTODIN II is depicted in Figure 1-1. A host subscriber hereafter referred to as the user need not implement the higher level Host-to-Host or Terminal-to-Host protocols to access the backbone. All that is necessary is the SIP and the Mode VI link procedure. SIP provides a set of procedures and rules by which to reliably exchange data and control information with the backbone (SCM in particular). SIP will accept user information, attach the appropriate leader and pass it to the Mode VI controller for transfer across the SIP-SCM access line. In the other direction SIP will receive information from the backbone, detach the leader and

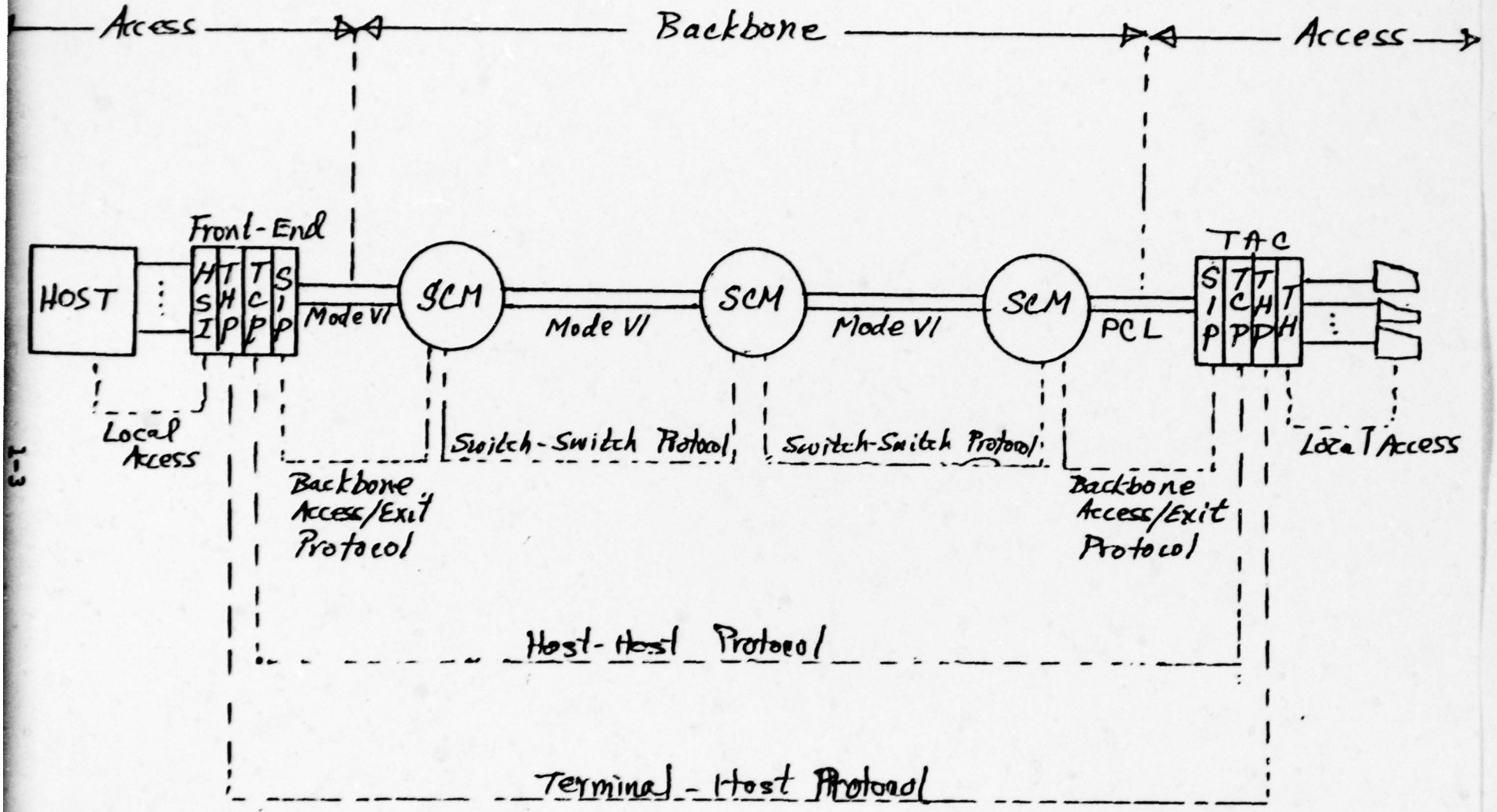


Figure 1-1 Autodin II Protocols

pass it to the user. The properties of SIP are listed in Figure 1-2 and explained below.

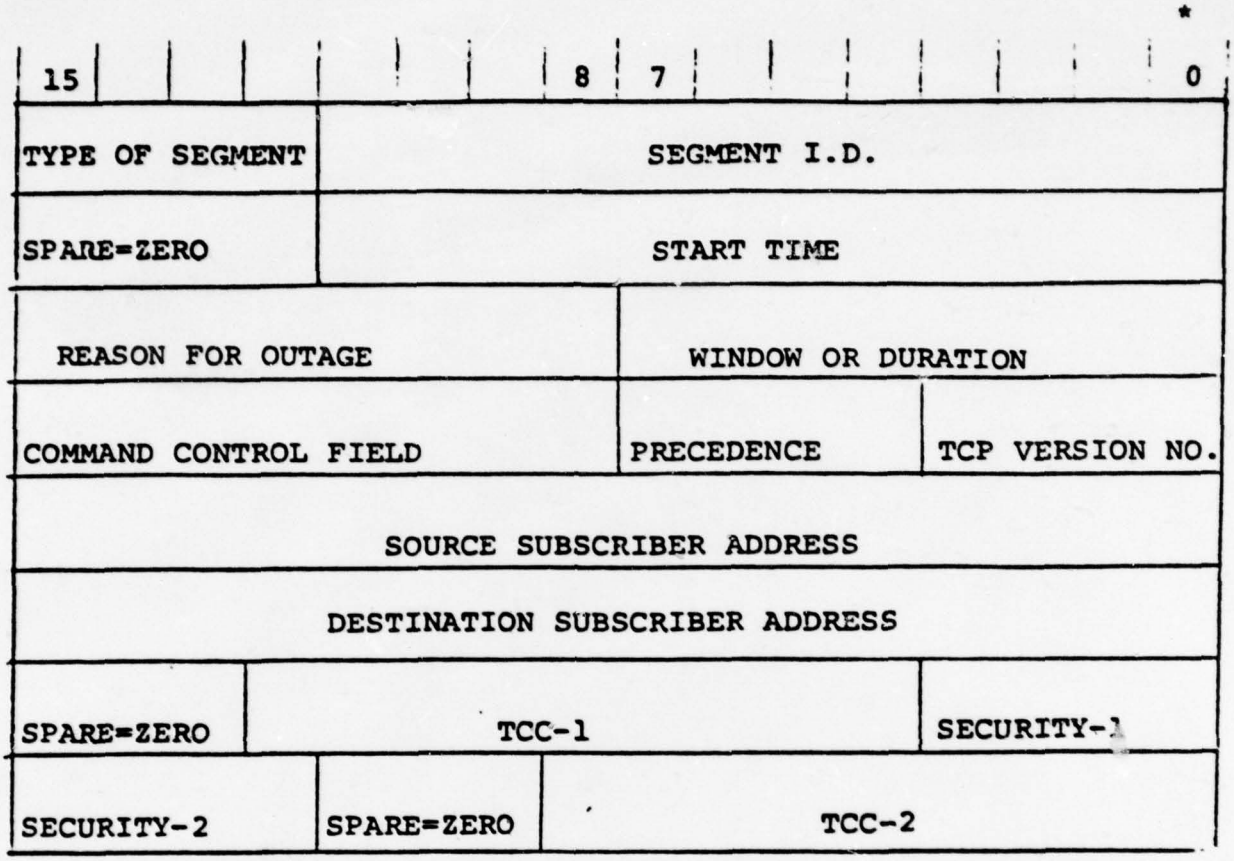
The information entities SIP transmits to and receives from the backbone are called segments. A segment is a completely self-contained unit of information as far as SIP and backbone handling are concerned. It will include in its header control information, source and destination addressing, security, precedence and Transmission Control Code (TCC); in essence everything the backbone requires to route it to its destination. The leader is called the Binary Segment Leader (BSL). See Figure 1-3.

Because of the independent handling of segments by both the backbone and SIP, relationship between a series of segments such as the order of presentation by the user may be lost. Adaptive routing and retransmissions within the backbone might cause out-of-order arrivals at the destination SIP. Also, since segments of differing precedence from multiple sources can arrive at the destination simultaneously, the SCM-to-SIP segment stream will be multiplexed and unordered. Further, under abnormal conditions (i.e. switch failure) the backbone may lose or duplicate segments, therefore, no guarantees against possible duplication, loss, or nonsequenced delivery to the destination SIP are made. Recovering lost segments, resequencing of out-of-order arrivals, demultiplexing segments from multiple sources and end-to-end accountability are the responsibilities of the end users or any higher level protocol acting in behalf of the end users. The backbone will, however, report back to the source SIP on a per segment basis if it knowingly fails to successfully deliver a segment to the destination or deliberately destroys a segment to relieve congestion. These backbone accountability messages are called Non-Delivery Notices (NDN).

The SCM will control the flow of segments from the SIP to it in order to provide an equitable sharing of its resources and to relieve possible congestion within the backbone. The control is exercised by a periodic window allocation which informs the SIP the number of segments it may transmit with minimal rejection. The SIP will also have the ability to request more

PROPERTIES	SIP TO SCM	SCM TO SIP
Unit of Transfer	Segment	Segment
Leader Type	Binary Segment Leader	Binary Segment Leader
Accountability	None	Non-Delivery Notices
Flow Control	None	Window
Recovery	Subscriber Status Notices	SCM Status Notices
Routing Data	Source and Destination Subscriber Addresses	Source and Destination Subscriber Addresses
Privacy Label	Security and TCC Designations	Security and TCC Designations
Testing	Echo	Echo

FIGURE 1-2 SIP PROPERTIES



* In the bit serial transmission across the interface, this is the first bit out.

GENERAL BINARY SEGMENT LEADER

FIGURE 1-3

Type of Segment	- This field is always set to zero by SIP and used by the network to tag segments for NCC reporting (e.g. trace). The field may, therefore,be filled in with a non-zero code on segments from the network.
Segment I.D.	- This field is used by SIP to uniquely identify all data segments and optionally to identify control segments. The network ignores this field. Any segment report (NDN, reject, etc.) on a data or control segment will be a return of the BSL with this field unchanged.
Spare	- All spare fields must be set to zero by both the SIP and the network.
Start Time, Duration, Reason for Outage	- These fields are parameters which must be set by SIP or network when using the "Going Inoperable" status subcommands.
Window	- This field is used by the network to pass the new data segment window (W) to the SIP. It is a parameter of the flow control command. The window value replaces any previous values of W. Each data segment which is passed from the SIP to the network decrements this window.
Command Control Field	- This field is used by both the SIP and network to distinguish between data and control segments and to identify control functions/services between the SIP and the network. Control segments never carry text (except the SCM initiated echo text). Controls are never piggybacked with data segments. See Figures 2-1 and 2-2.
Precedence	- This field identifies the precedence handling and protection level at which the segment (control or data) should be handled. See Figure 2-5.
TCP Version Number	- This field identifies the originating SIP's user (TCP, other high level protocol, utility, etc.). It is ignored by the network and is used by the destination SIP to pass the segment on to the proper higher level protocol.
Source Subscriber Address	- This field is the originating SIP's logical address. This is the single, unique host level logical address associated with the SIP and its access line.
Destination Subscriber Address	- This field is the destination SIP's logical address. All SIPs have only one logical address which is used for both source and destination labling.

GENERAL BSL FIELD DESCRIPTIONS

FIGURE 1-3 (Cont'd)

TCC (1&2) - The TCC-1 field identifies the Transmission Control Code (privacy code) which designates the privacy handling which the network must give to the segment. All segments must be labeled with an authorized TCC. The TCC-2 Field is a redundant exact duplicate of TCC-1. The TCC is assigned by the source SIP and delivered intact to the destination.

Security (1&2) - The Security-1 field designates the security level at which the network must handle the data segment text. All segments must be labeled with an authorized security level. The Security-2 field is a redundant exact duplicate of Security-1. The security level is assigned by the source SIP and delivered intact to the destination.

NOTE: Specific binary patterns for security, TCC and address field entries are available upon request from DCA Code 530, Washington, DC 20305.

GENERAL BSL FIELD DESCRIPTIONS

FIGURE 1-3 (Cont'd)

window space in the event the SCM does not automatically update the window or the SIP exhausts its window supply quickly.

SIP's recovery procedures are minimal since segment sequence synchronization procedures aren't required. The segment I.D. may or may not be assigned consecutive sequence numbers. Its only purpose is for the user to identify a segment uniquely. Therefore synchronization on what sequence number the SIP will begin transmitting at and the SCM will receive at is unnecessary. Other recovery aspects include the ability of the SCM and SIP to each declare its own status i.e., Operable or Inoperable.

A data segment transmitted by SIP to the SCM will contain source and destination subscriber addressing. In the SCM, the segment is converted to a packet by adding the source and destination SCM addressing. It is routed based on these addresses to the proper destination SCM where the packet is reconverted to a segment and transmitted on the destination SIP's access line.

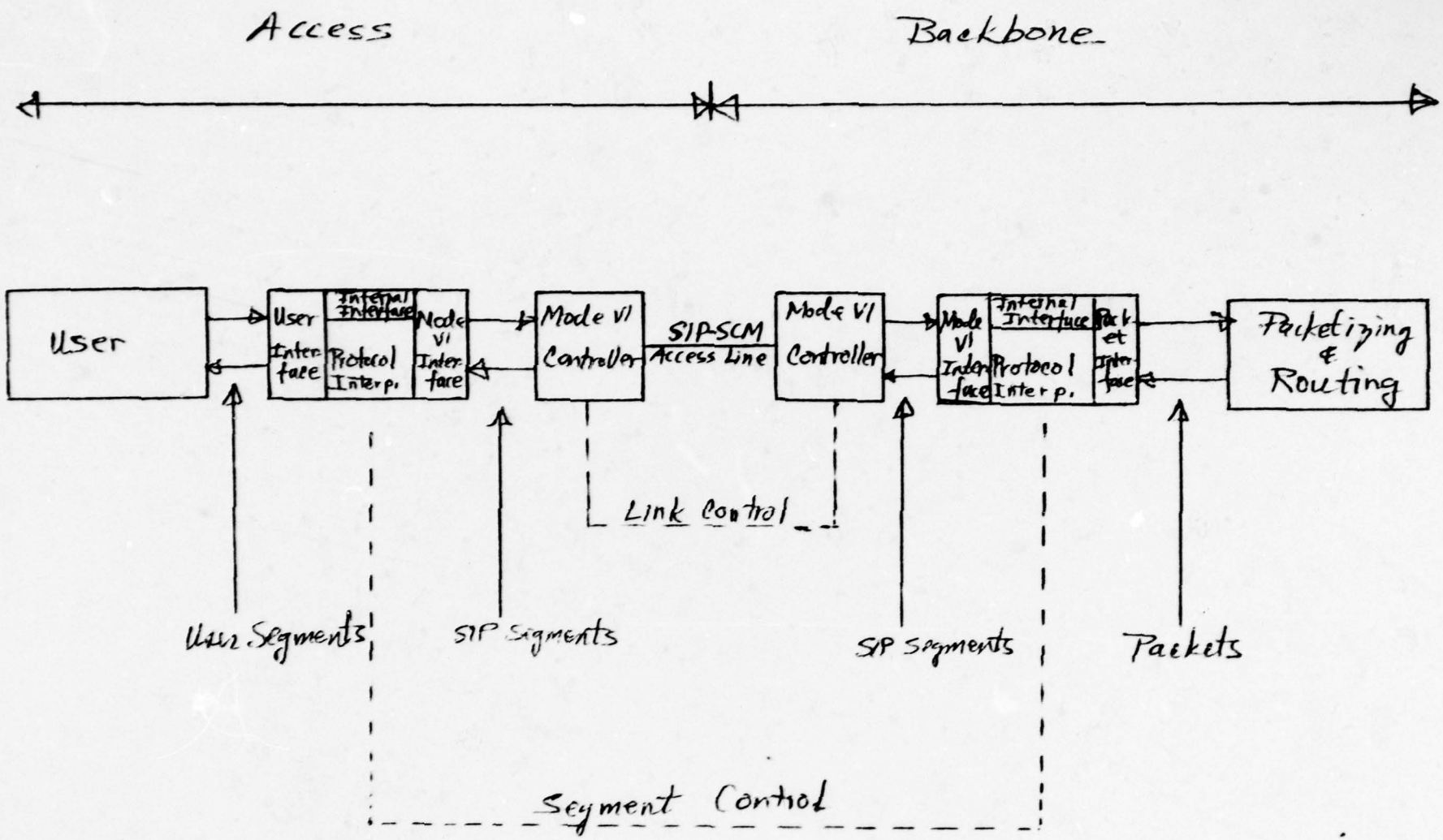
Each segment will also contain privacy information consisting of security and TCC designations. These codes are validated at the source SCM before acceptance and at the destination SCM before delivery.

The Echo feature is in SIP to allow online testing of the SIP-SCM access line.

1.2 SIP Architecture

SIP is organized into four major sections: the User Interface, the Internal Interface, the Mode VI Interface and the SIP/SCM Protocol Interpreter. These sections and their counterparts at the SCM are depicted in Figure 1-4.

The User Interface exchanges with the User Program entities called user-segments. A user-segment consists of user text and segment parameters. The parameters are security, TCC, precedence, destination subscriber address and a segment ID. These parameters along with a few others are encoded into the BSL by the Protocol Interpreter of SIP and then passed on to the Mode VI



General SIP Architecture

Figure 1-4

controller by the Mode VI Interface. Notice the layered architecture of the link and segment protocols. The link protocol's only responsibility is to reliably exchange information across the transmission medium whereas SIP's major function is to reliably exchange segments with sufficient information included to allow the backbone to verify, route and deliver the segments out of the backbone.

The major SIP data flows are depicted in Figure 1-5.

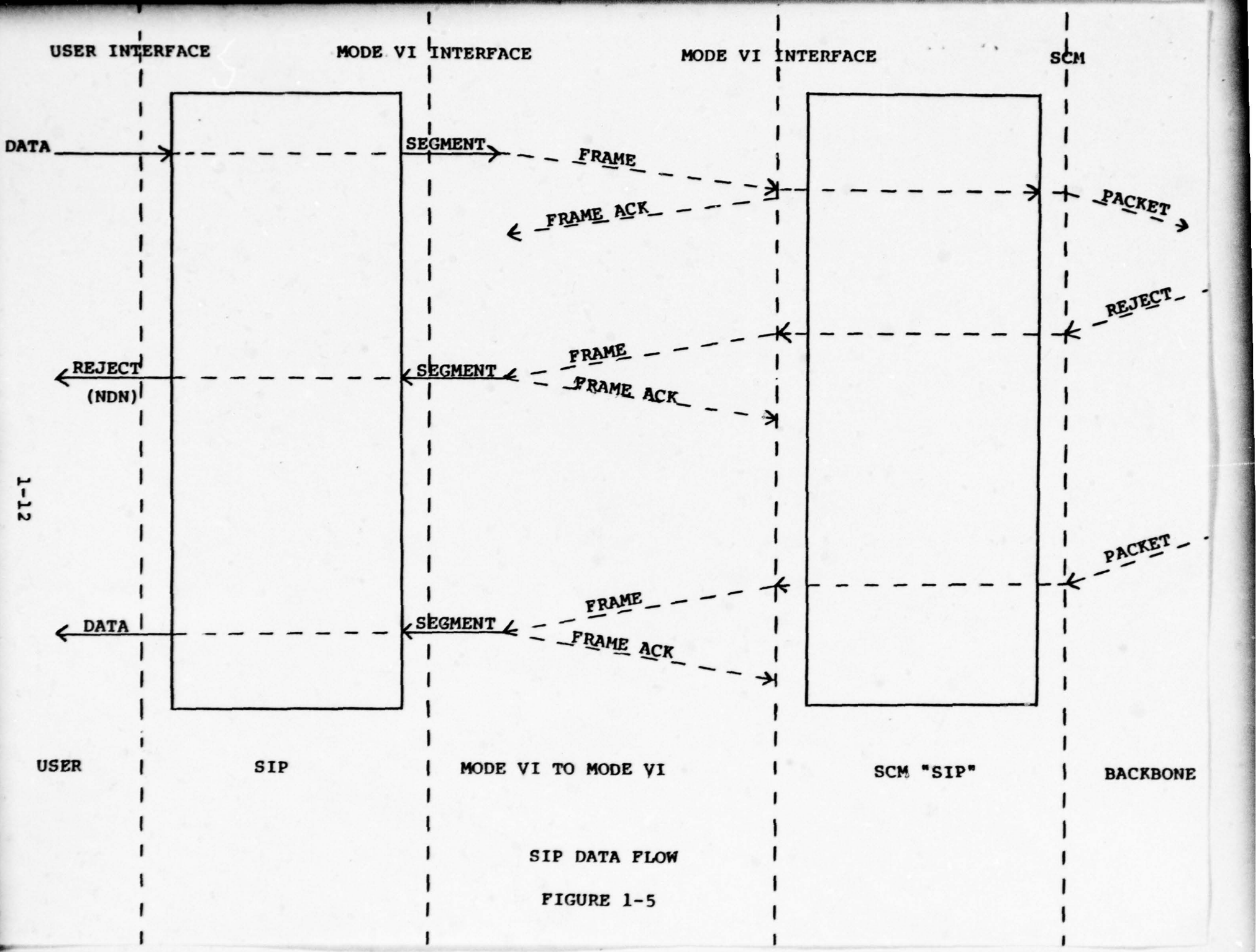
The remainder of this document only specifies the stimuli/response functions of the host SIP interpreter. These are the functions which will be tested and certified before a subscriber host is permitted to operate on the network. The internal SIP interfaces are purely host unique and are therefore not specified.

The description of the SIP interpreter functions is from the point of view of the host SIP. These descriptions in Section 2 are high level functional definitions of a SIP interpreter software module.

1.3 Functional Interaction Between SIP and Mode VI

There are a few minimal functional couplings between the SIP and the Mode VI link level protocol. These couplings are required in order for the host/backbone interface to operate as a system:

- Each segment must be totally carried in a Mode VI frame with no other segments. A segment always starts with a full (128 bit) BSL followed by zero (for controls) to 4992 bits of user data.
- Control segments must be processed first-in-first-out (FIFO) through both SIP and Mode VI to keep both SIP and SCM in synchronization. Non-control segments may be processed in any order by SIP, but Mode VI must process them FIFO as received, since the Mode VI Ack serves as the SIP Ack.



SIP DATA FLOW

FIGURE 1-5

- The SIP Interface Down state must be coupled to the Mode VI Receiver Not ready (RNR) state. That is if the SIP transitions to Interface Down then the Mode VI must transition to Mode VI RNR. They must similarly make the same coupled transitions out of these states. Temporary Mode VI RNR conditions (such as exhaustion of Mode VI sequence numbers or buffer space) should not be coupled to SIP Interface Down state, rather persistent Mode VI problems must be coupled back to SIP. The Mode VI may transition to deeper states of inoperability once the SIP is in the Interface Down state. The only fatal coupling condition is the SIP in Interface Down state while the Mode VI is still accepting segments. The equivalent state coupling is true in the SCM. This is because the Mode VI ACK is assumed by the switch to indicate successful reception by the user.

SECTION 2

PROTOCOL INTERPRETER

The Protocol Interpreter part of SIP is responsible for implementing precise data and control transfer procedures to reliably exchange segments between the SCM and SIP. Every segment exchanged across the SIP-SCM access line has appended to it a 128 bit Binary Segment Leader (BSL). The BSL is essentially the carrier of the protocol with fields specifying the command, related parameters, security, TCC, precedence, and addressing. The complete set of commands are listed in Figures 2-1 and 2-2. Data segments from the User are appended BSLs containing the user supplied source and destination subscriber addresses, security, TCC, precedence and the user segment identification. The segment is passed to the Mode VI controller for transmission if a non-zero window exists. The window reflects the number of segments the SCM is willing to receive with minimal rejection. A zero window causes the segment to be held temporarily until either the holding period has expired or the SCM has updated the window. An updated window will cause the held segment to be transmitted to the SCM, whereas a holding period expiration will cause a message to be returned to the user indicating the segment was blocked due to SCM flow control.

Several commands exist which control SIP to SCM segment flow. These are Request Window, Subscriber Status and the Echo commands. Request Window allows SIP to request window space from the SCM such that temporarily held segments can be transmitted. The Subscriber Status commands inform the SCM of a change in user status.

Data segments received from Mode VI controller and therefore from the SCM require minimal processing. They are first validated and then passed on for delivery to the User.

Control segments received from the SCM can be classified as Reject Notices, Window Update (Ready for Next Segment),

COMMAND		SUBCOMMAND		PARAMETERS
BIT POS.		BIT POS.		
15-11	DESCRIPTION	10-8	DESCRIPTION	
00000	(Not Used)	000		
00001	Data	000	None	
00010	Echo	001	Reply	
00011	(Reserved)			
00110	Request Window	000	None	
01101	Subscriber Status	000	Subscriber Going Inoperable	Start Time, Duration, Reason
		001	Subscriber Operable	
		010	Subscriber Access Circuit Going Inoperable	Start Time, Duration, Reason
		011	Subscriber Busy	

SIP - TO - SCM COMMANDS

FIGURE 2-1

COMMAND		SUBCOMMAND		PARAMETERS
BIT POS.		BIT POS.		
15-11	DESCRIPTION	10-8	DESCRIPTION	
00000	(Not Used)	000		
00001	Data	000	None	
00010	Echo	000	Request	
00011	(Reserved)			
00100	Flow Control	000	Ready for next Segment	Window
00101 00110 00111	(Not Used)			
01000	Non-Delivery Notice (Flow Control)	000	Blocked at the Source-Traffic Acceptance Category too low	
		001	Rejected, beyond Global Window	
		010	Rejected, Congestion at Source SCM	
		011	Rejected, Congestion at a Backbone Trunk	
		100	Rejected, Congestion at the Destination Access Line	
01001	Error Reject	000	Invalid BSL	
		010	Illegal Command Code	
01010	Non-Delivery Notice (Undeliverable)	000	Destination Subscriber Down	
		001	Destination Subscriber Circuit Down	
		010	Destination Subscriber Busy	
		011	Network Discard	
01011	Validation Reject (any SCM)	000	Invalid Security	
		001	Invalid TCC	
		010	Invalid Address	
		011	Invalid Precedence	
01100	SCM Status	000	SCM Going Inoperable	Start Time, Duration, Reason
		001	SCM Operable	

SCM - TO - SIP COMMANDS

FIGURE 2-2

COMMAND		SUBCOMMAND		PARAMETERS
BIT POS.		BIT POS.		
15-11	DESCRIPTION	10-8	DESCRIPTION	
		010	Access Line Going Inoperable	Start Time, Duration, Reason
		011	Access Line Operable	
		100	SCM Busy	
01101	(Reserved)			
01110 THRU 11111	(Not Used)			

SCM - TO - SIP COMMANDS (Cont'd)

FIGURE 2-2

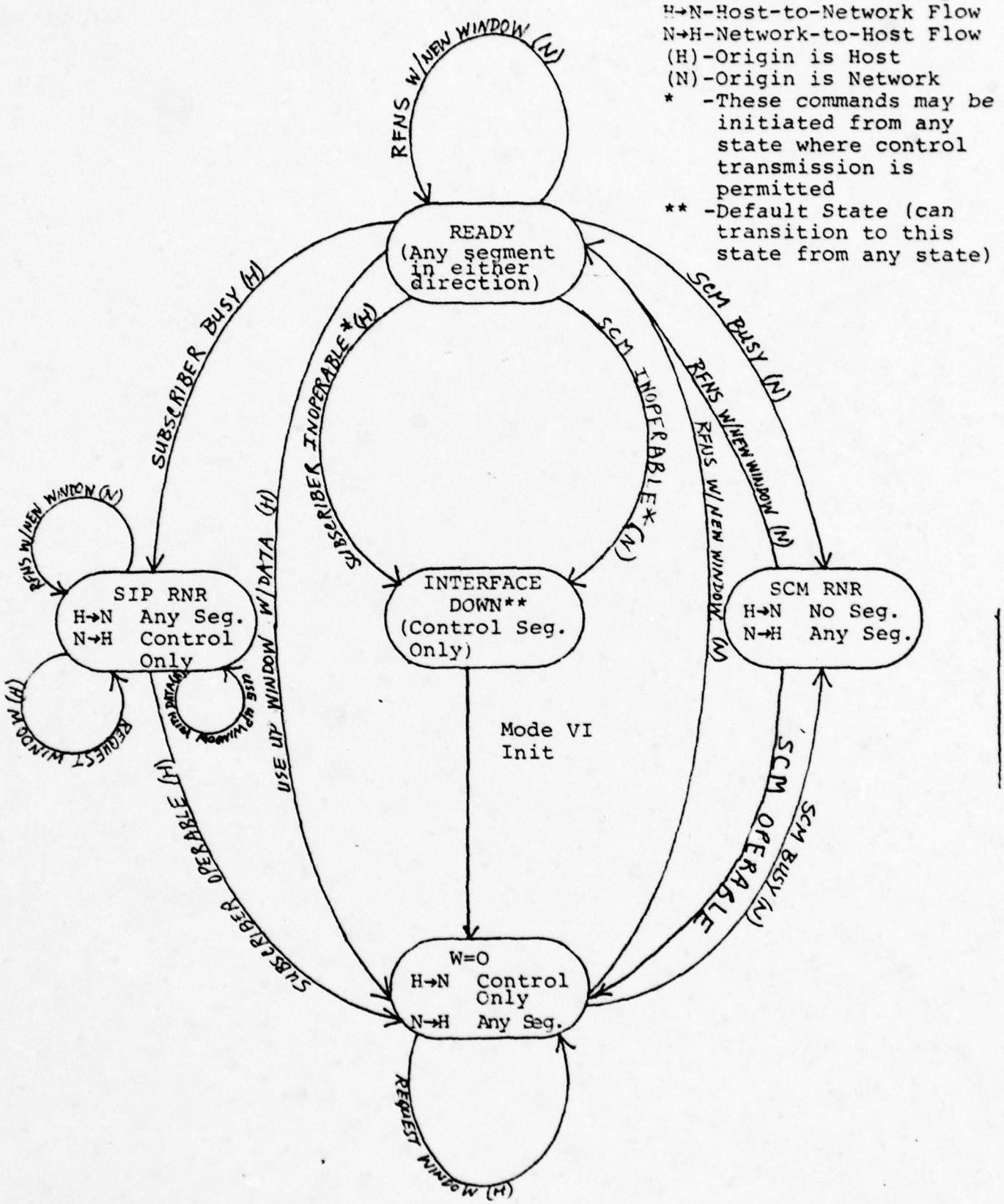
SCM Status Message and the Echo commands. Reject Notices refer to a particular segment that the backbone was unable to deliver to the destination subscriber. The Ready for Next segment updates the SIP window, thereby controlling the rate at which SIP can transmit segments to the SCM. The SCM status message indicates a change in SCM status. The echo functions exist for testing purposes only.

2.1 SIP State Description

The protocol aspects of SIP can be modelled and completely described by a five-state protocol diagram. The general SIP state diagram is depicted in Figure 2-3. It is not intended to be complete in detail; specifically, all state transitions are not shown. Complete detail is contained in Section 3. A brief description of the SIP states follows.

In the READY state segments can flow in either direction. User segments are appended BSLs and transmitted to the SCM. Data segments from the SCM are stripped of their BSLs and delivered to the User. The flow of segments from the SIP to the SCM is controlled by the SCM by periodic window allocations via the RFNS command. SIP can move to the INTERFACE DOWN state if either end of the line goes inoperable or the line itself fails. Either the SCM or SIP can declare himself busy and move SIP to the SCM RNR or SIP RNR state. These RNR states are not to be confused with Mode VI RNR. From the READY state SIP moves to the W=0 (Window= Zero) state once the window is depleted.

In the W=0 state, data segment flow (not control segment flow) is not allowed in the SIP-to-SCM direction although user segments are held in SIP allowing for the condition to clear up if at all possible. In the opposite direction, SCM-to-SIP, segments are processed as in the READY state. In this W=0 state, SIP can request for a window update via the Request Window command if the SCM fails to update in its periodic fashion. However, the likely explanation for SIP being in this state is that this subscriber is exhausting his equitably allocated window too quickly or is the cause of congestion within the backbone. In both cases



SIP STATE DIAGRAM

FIGURE 2-3

the throttling is purposeful and transmission of excessive Request Window commands will cause the SCM to respond with an SCM Busy status moving SIP to the SCM RNR condition.

In the SCM RNR state, the SCM will discard without returning Non-Delivery Notices any segment transmitted by SIP. However, segment flow in the opposite direction, SCM-to-SIP, is still in force.

The SIP RNR state is almost the opposite of the previous state except that the SCM is allowed to send controls to the SIP such as replenishing the window allocation. Segment flow from the SIP-to-SCM is processed as in the READY state.

The INTERFACE DOWN state is the default state (initial state) of SIP. The only events permitted in this state are Mode VI Initialization in either direction, and the Subscriber Operable control segment from SIP to the SCM. This state is actually the combination of several states: SIP DOWN and SCM READY, SIP READY and SCM DOWN, SIP DOWN and SCM DOWN, and SIP RNR and SCM RNR. This state is the initial state of SIP from a previous SIP down condition. Normally the end that moves SIP to the INTERFACE DOWN condition is responsible for moving SIP out of that state, but as part of the initialization process the SIP sends the SCM a Subscriber Operable command, since history of who initiated the down state is lost. Likewise, the SCM will send an SCM operable command when the SCM begins initialization.

2.2 Segments to the SCM

The following functions manage the transfer of data and control segments to the SCM. A 128-bit Binary Segment Leader (BSL) is appended to data segments from the user. Controls and associated parameters are coded in the proper BSL fields. All of the fields are not used for all segments. In particular, the Start Time, Duration, and Reason Code fields are used only for the Subscriber Status command. All non data segments are considered control segments. No control functions piggyback on data segments.

2.2.1 Data Segment to SCM Processing

This function will be responsible for processing data segments from the User. In the SIP RNR and READY states, user segments are appended a BSL and released to the Mode VI controller. The window is decremented by one for each data segment only (control segments do not decrement window). If the window reduces to zero, SIP moves to the W=0 state. A user segment is held in queue if SIP is in the W=0 state. In the SCM RNR and INTERFACE DOWN states user segments are not processed for transmission to the backbone, but are either discarded or returned to the User with an appropriate cause (either SCM Busy or Interface Down).

The proper coding of the BSL is explained below and depicted in Figure 2-4.

Type of Segment Field - This field is set to zero for all segments in the SIP-to-SCM direction.

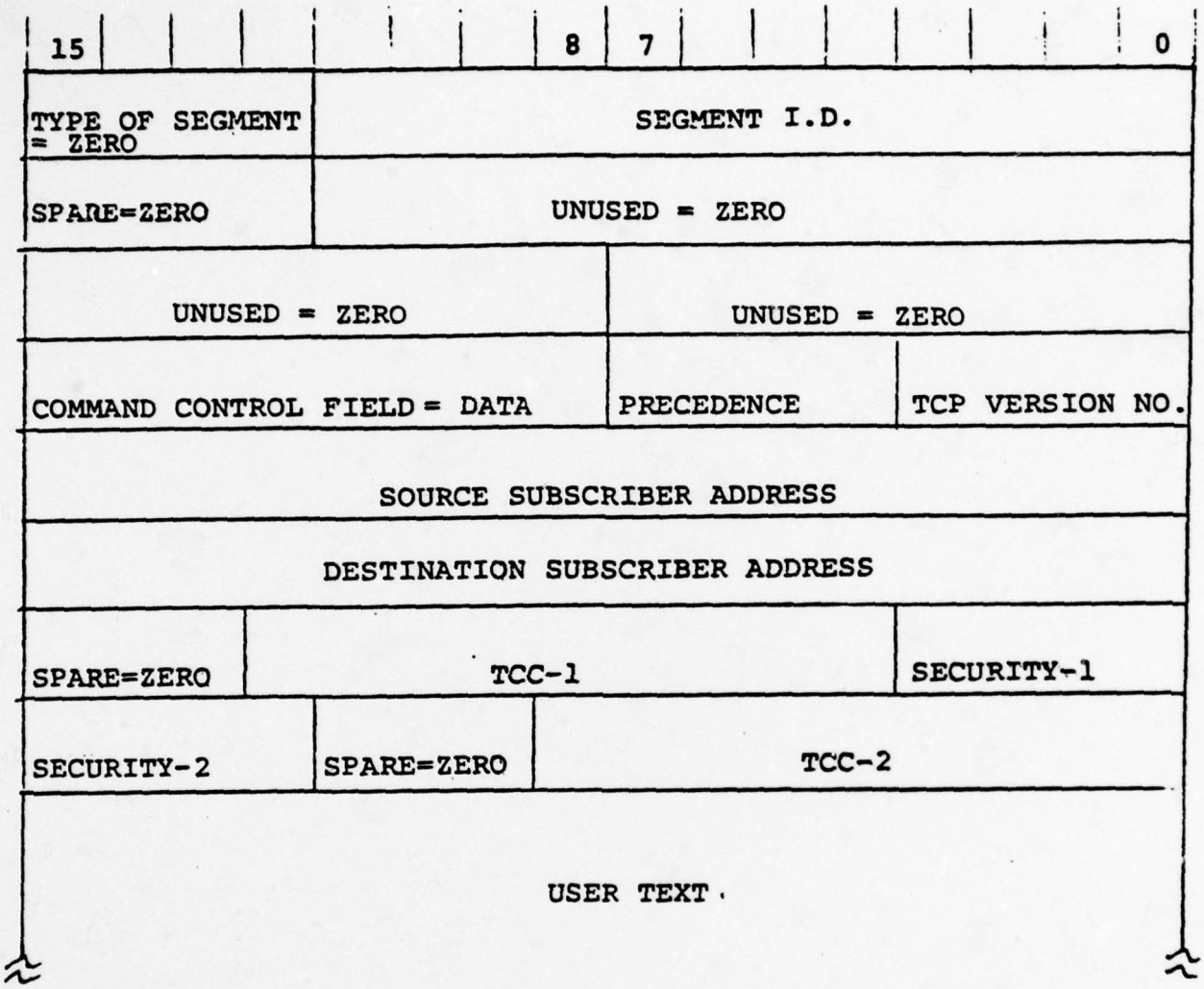
Segment I.D. Field - Segment identification provided by the User is placed in this field. The segment I.D. is used by SIP to uniquely identify a segment.

Unused and Spare Fields - All unused and spare fields are set to zero.

Command Control Field - This field is coded as data. It indicates that the segment contains text following the BSL.

Precedence Field - The precedence associated with the segment is coded into precedence field. This will indicate to the backbone the urgency of the segment. High precedence segments will normally get priority in both processing and resources in the backbone. The SIP to SCM access line will be authorized a ceiling precedence level above which it cannot assign to segments. If the precedence exceeds the ceiling level, the SCM will return a validation reject with the appropriate cause. The precedence codes are listed in Figure 2-5.

TCP Version No. Field - The TCP Version Number of the User allows for the identification of different versions of TCP that



SIP - TO - SCM DATA SEGMENT

FIGURE 2-4

USER CATEGORY		BIT POSITIONS 7	6	5	4	DESCRIPTION
CAT I	I-1	1	1	1	1	NETWORK ONLY
	I-2	1	1	1	0	NETWORK ONLY
	I-3	1	1	0	1	CRITIC/ECP
	I-4	1	1	0	0	FLASH, I/A,Q/R,N/R, & BULK
CAT II	IIA	1	0	1	1	I/A
	IIB	1	0	1	0	Q/R
	IIC1	1	0	0	1	BULK 1/NARRATIVE
	IIC2	1	0	0	0	BULK 2
CAT III	IIIA	0	1	1	1	I/A
	IIIB	0	1	1	0	Q/R
	IIIC1	0	1	0	1	BULK 1/NARRATIVE
	IIIC2	0	1	0	0	BULK 2
CAT IV	IVA	0	0	1	1	I/A
	IVB	0	0	1	0	Q/R
	IVC1	0	0	0	1	BULK 1/NARRATIVE
	IVC2	0	0	0	0	BULK 2

NOTES: 1. The combination of bits in positions 7 and 6 uniquely define the user precedence category,

2. The combination of bits in positions 5 and 4 uniquely define the subcategory within each category.

LEVELS OF PRECEDENCE

Figure 2-5

may exist at the user side of SIP. The code for the AUTODIN II TCP is one. The code for no TCP is zero. All other codes are reserved and will be assigned by DCA Code 530.

Source Subscriber Address Field - The subscriber address of the host accessing AUTODIN II via this SIP is placed in this field.

Destination Subscriber Address Field - The address of the subscriber to which this segment is destined is placed in this field.

Security Fields - The security assigned by the User to this segment is inserted in both fields. The user text will be handled at the security level assigned by the SIP. The security field allows up to 16 security designations. The redundant security field is present to provide the means to detect store/fetch malfunctions.

TCC Fields - The TCC code assigned by the User to this segment is inserted in both fields. The TCC provides a means to partition traffic and define controlled communities of interest among subscribers. A redundant TCC field provides the same malfunction protection as provided by the redundant security field.

2.2.2 Request Window Processing

Request for Window processing can take place only in the W=0 state and SIP RNR state with window depleted. When a user segment is processed and transmitted to the SCM, the window is reduced by one. If the window is reduced to zero, then a timer is set to approximately the value of the SCM's window update period. A Request Window command is sent to the SCM if the timer expires and the SIP state is either SIP RNR with window still zero or W=0. A timer expiration with SIP in any other state is ignored and indicates that either the SCM has updated the window or some other stimulus has moved SIP to another state. The Request Window can be retransmitted (upon successive timer expirations) up to five times if no responses are received from

the SCM. After the fifth unsuccessful attempt, the SCM is assumed to be down or busy and SIP moves accordingly to the INTERFACE DOWN state if in the SIP RNR state or to the SCM RNR state if in W=O state.

The proper coding of the BSL is explained below and depicted in Figure 2-6.

Type of Segment Field - This field is set to zero.

Spare and Unused Fields - All unused and spare fields are set to zero.

Command Control Field - This field is coded as Request Window.

Precedence Field - All SIP-to-SCM controls are assigned the maximum allowable precedence the SIP-to-SCM access line is authorized to carry.

Source Subscriber Address Field - The subscriber address of the host accessing AUTODIN II via this SIP is placed in the field.

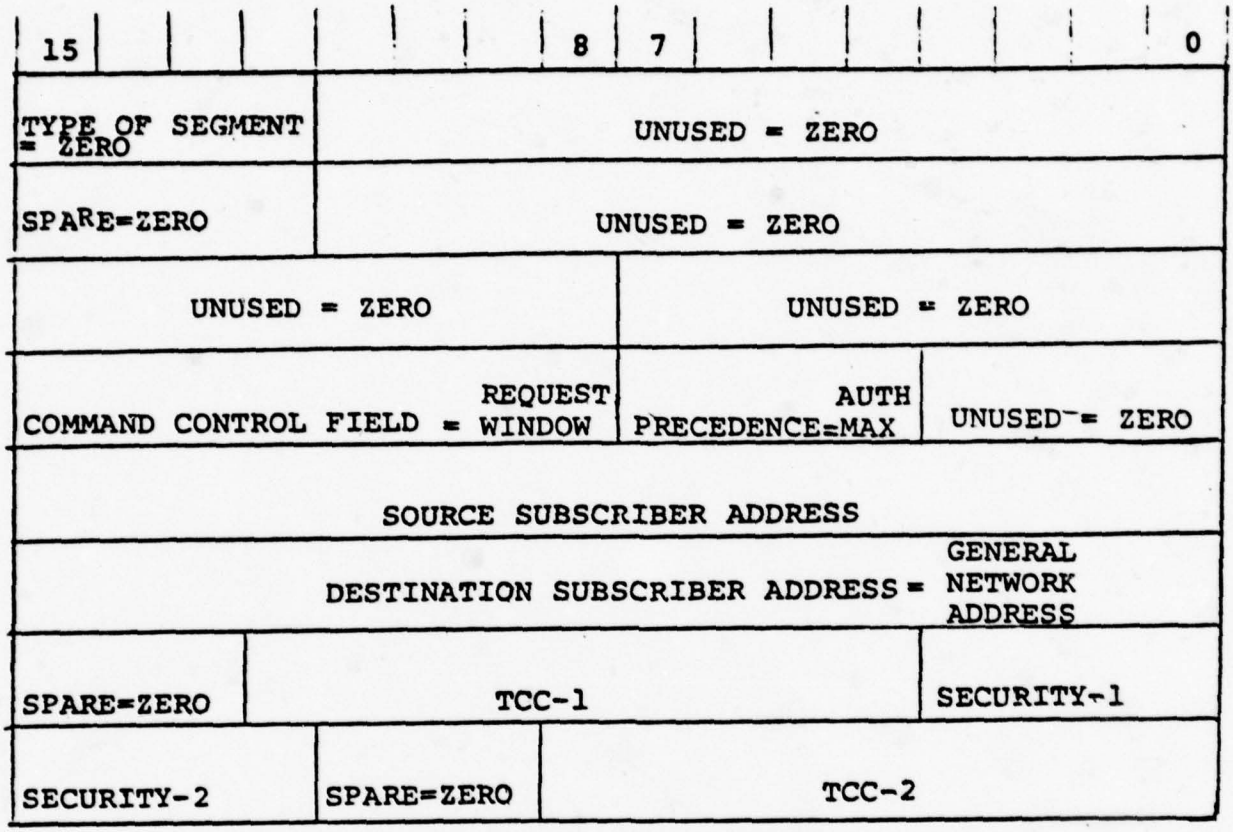
Destination Subscriber Address Field - The AUTODIN II backbone is assigned a general network address. This address is placed in this field.

Security Fields - Any authorized security level of this SIP's subscriber is placed in these fields.

TCC Fields - Any authorized TCC designation of this SIP's subscriber is placed in these fields.

2.2.3 Subscriber Status Processing

The Subscriber Status command has four subcommands specifying the status. These status messages are sent to the SCM (from any state except SCM RNR) only if a change in the present or future status of the subscriber is to take place. The Subscriber Going Inoperable and Subscriber Access Circuit Going Inoperable subcommands move SIP to INTERFACE DOWN state at the time indicated in the parameter field. After the duration of inoperability,



SIP - TO - SCM REQUEST WINDOW SEGMENT

FIGURE 2-6

the Subscriter Operable subcommand is sent and SIP moves to the W=O state. From this state SIP moves to the READY state after the SCM updates the window with the RFNS command. When the Subscriber Busy subcommand, indicating that the subscriber is temporarily unable to handle any more data, is sent to the SCM, SIP moves to the SIP RNR state from all other states except SCM RNR and INTERFACE DOWN states. In these states SIP moves to the INTERFACE DOWN state. The SCM on reception of the Subscriber Busy subcommand will inhibit all data segment transmission to the SIP.

The proper coding of the BSL is explained below and depicted in Figure 2-7.

Type of Segment Field - This field is set to zero.

Unused and Spare Fields - All unused and spare fields are set to zero.

Start Time - This field is unused except for the "Going Inoperable" subcommands. For these subcommands, the time that the INTERFACE DOWN condition will begin is indicated by the number of minutes (binary number in the Start Time field) from the current time.

Duration - This field remains unused except for the "Going Inoperable" subcommands. For these subcommands, the duration of the down condition is indicated by a number of minutes binary number.

Reason - This field contains the cause for the impending down condition. The only reason for outage thus far identified is scheduled maintenance (code = zero).

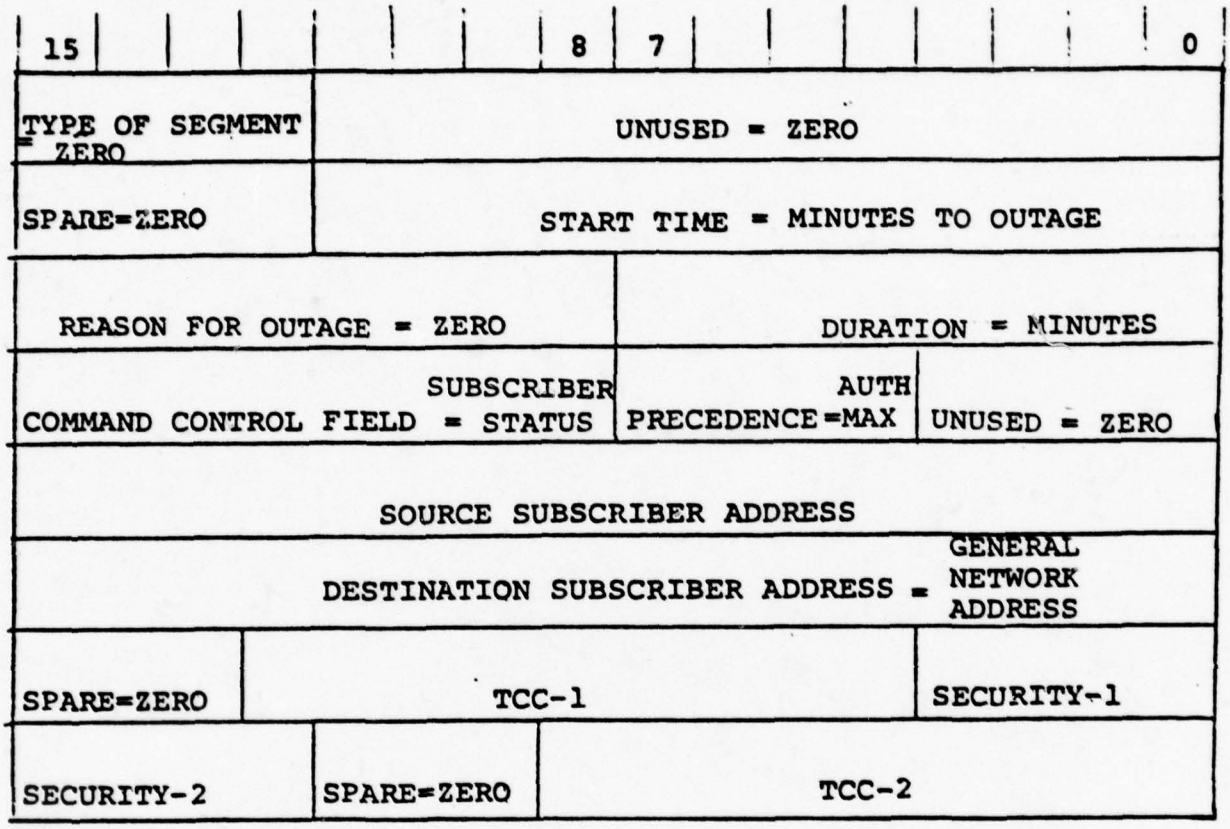
Command Control Field - The particular status code is inserted in this field.

Precedence Field - As in all control segments, the maximum authorized precedence level is assigned.

Source Subscriber Address Field - The subscriber address of the host accessing AUTODIN II via this SIP is placed in this field.

Destination Subscriber Address Field - The general network address is placed in this field.

Security Fields - Any authorized security level of this SIP's subscriber is placed in these fields.



SIP - TO - SCM SUBSCRIBER STATUS SEGMENT

FIGURE 2-7

TCC Fields - Any authorized TCC designation of this SIP's subscriber is placed in these fields.

2.2.4 Echo

The Echo data segment, used for testing purposes, can be sent in only the READY state. It expects the SCM to return the entire self addressed segment. The Echo Reply subcommand is the response for the SCM's echo request and is only sent in the READY state.

The proper coding of the BSL is explained below and depicted in Figures 2-8 and 2-9.

Type of Segment Field - This field is set to zero for the echo request. For Echo Reply the field is left unchanged from that of the SCM's echo request format.

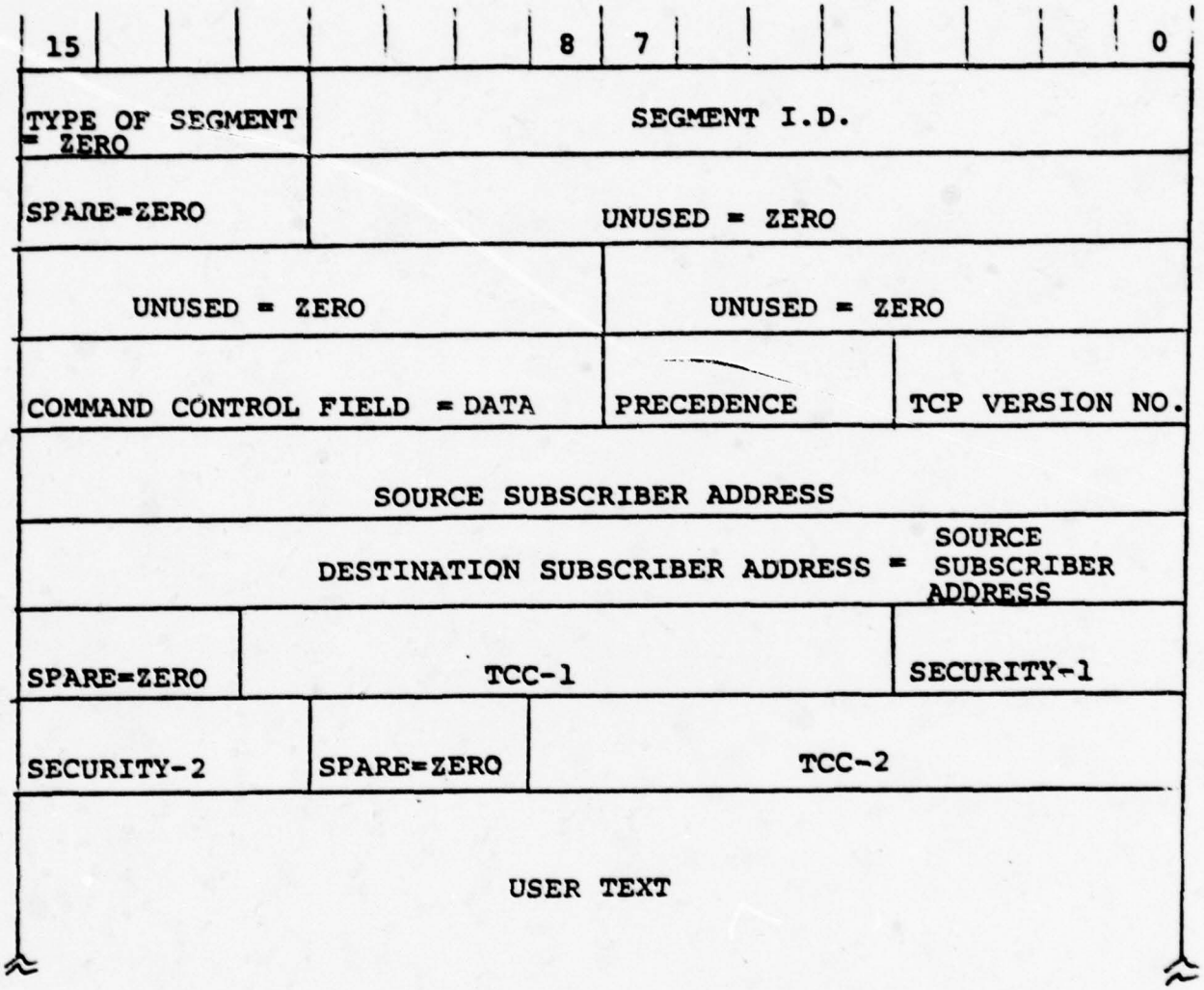
Segment I.D. Field - This field is coded and interpreted in the same manner as any other data segment for echo request. For Echo Reply the field is left unchanged from the SCM's echo request format.

Unused and Spare Fields - These fields are set to zero.

Command Control Field - This field is set to data for echo request and to Echo Reply for the Echo Reply.

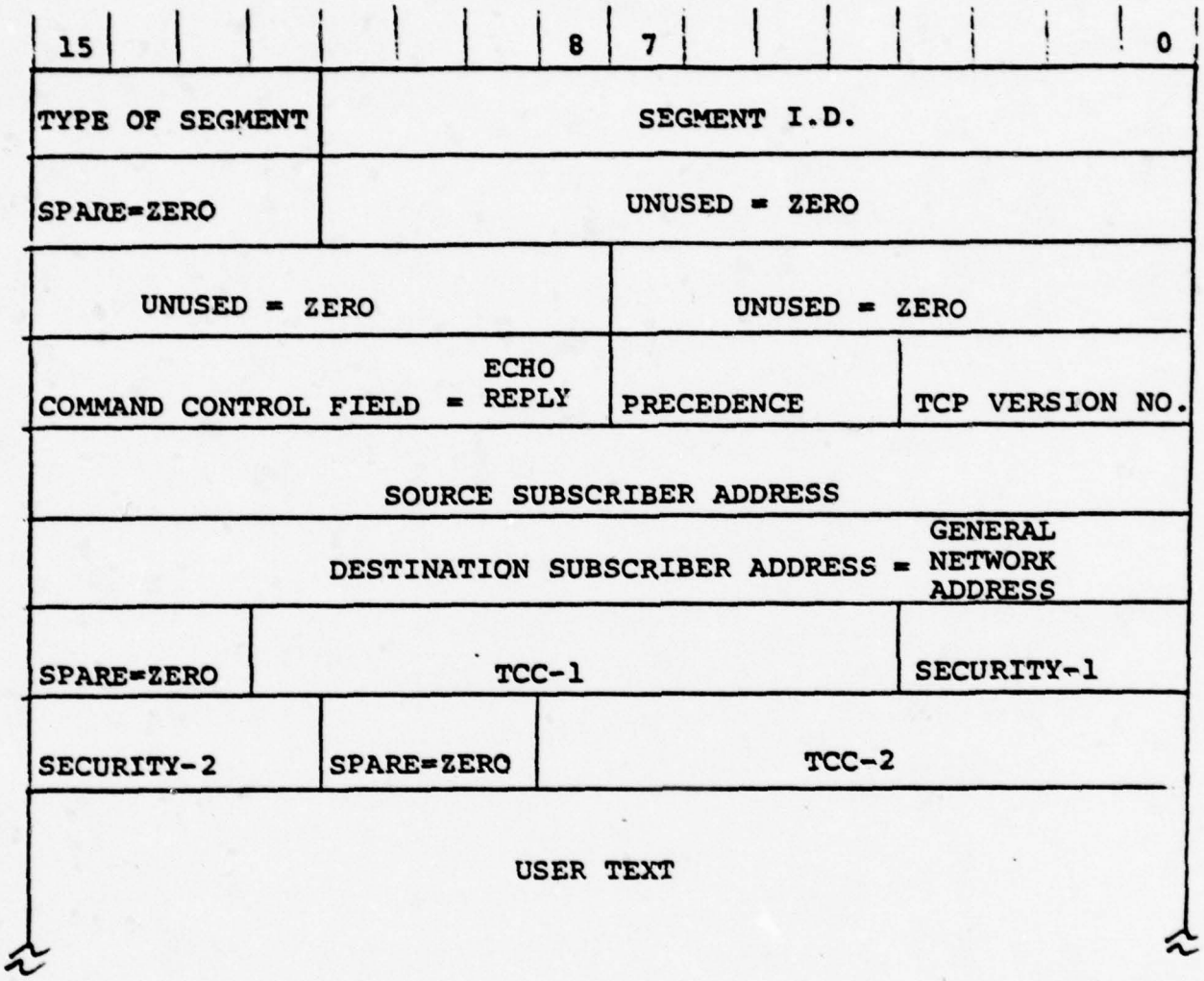
Precedence Field - For the echo request any precedence level authorized for the SIP-SCM access line may be placed in this field. If the User is originating the echo request, the precedence assigned by User is placed in this field as long as it lies within the ceiling authorized. For the Echo Reply the precedence field setting is unchanged from that of the SCM's echo request.

TCP Version No. Field - For the echo request the field is set to the value assigned by the User if the User originated the echo segment or to any value if SIP originates the echo segment. The field is left unchanged for the Echo Reply from that of the SCM's echo request.



SIP - TO - SCM ECHO REQUEST DATA SEGMENT

FIGURE 2-8



SIP - TO - SCM ECHO REPLY SEGMENT

FIGURE 2-9

Source Subscriber Address Field - The SIP's subscriber address is placed in this field for both Echo Request and Echo Reply.

Destination Subscriber Address Field - This field is set to the source subscriber address (self addressed) for the Echo Request. This field is set to the general network address for the Echo Reply.

Security Fields - These fields may be set to any authorized security level.

TCC Fields - These fields may be set to any authorized TCC designation.

2.3 Segments From the SCM

The following functions manage the transfer of data and control segments from the SCM. A 128-bit Binary Segment Leader(BSL) has been appended to data segments from the SCM. Controls and associated parameters are coded in the proper BSL fields. All of the fields are not used for all segments. In particular, the Start Time, Duration, and Reason Code fields are used only for the Subscriber Status command. All non data segments are considered control segments. No control functions piggyback on data segments.

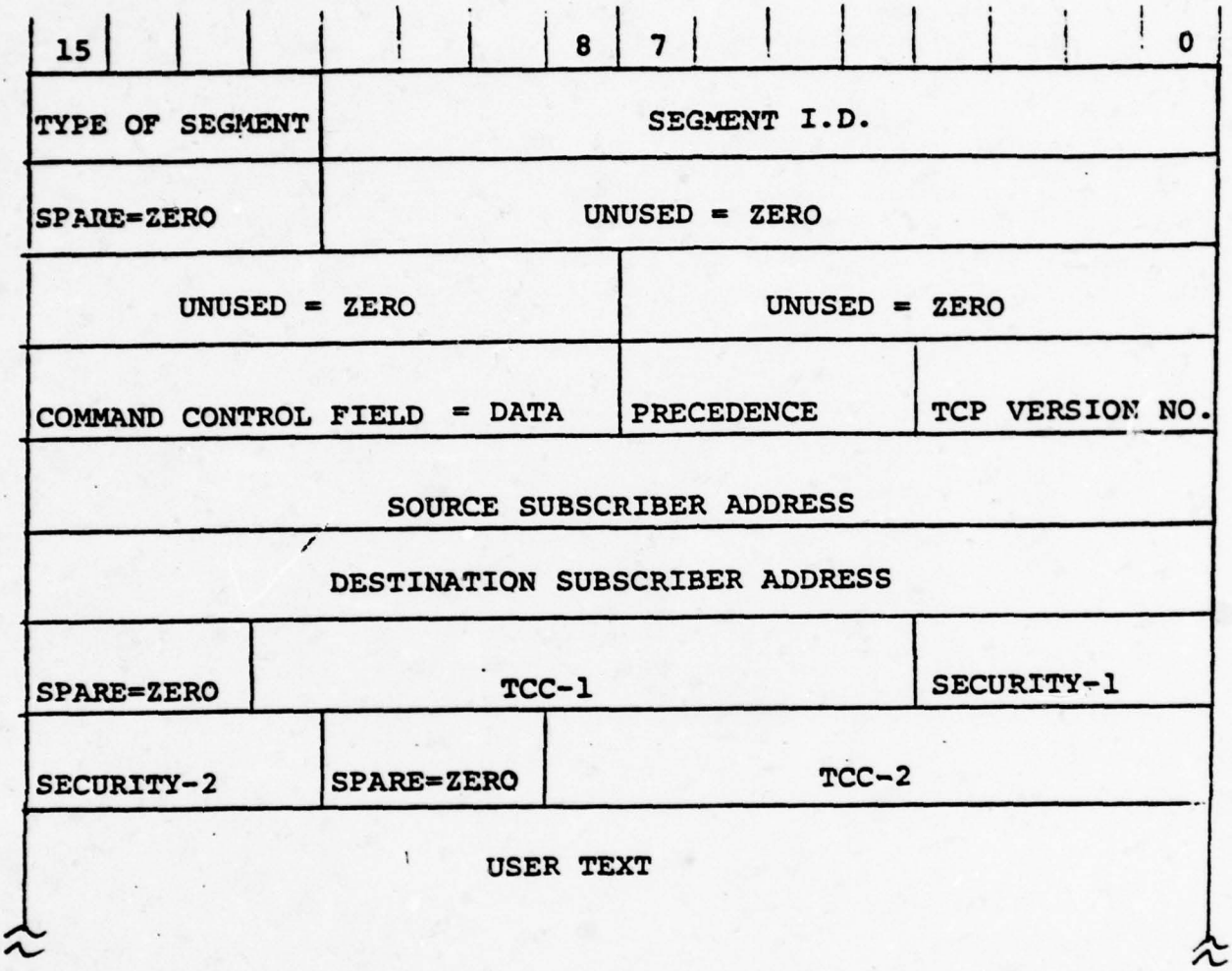
2.3.1 Data Segment

A data segment from the SCM is accepted in the READY, W=O and SCM RNR states only. Data segments received in the other two states are discarded. The BSL is validated by the SIP for proper format.

The proper format of the received BSL is explained below and depicted in Figure 2-10.

Type of Segment Field - The settings in this field are ignored by the SIP.

Segment I.D. - The segment I.D. identifies the segment for the source transmitting the segment and is mainly used to report back to the source if the segment is rejected in the backbone. To the destination subscriber this field might have no meaning, but the end users might desire to use the segment I.D. field for end-to-end purposes. Therefore, the segment I.D. field is passed to the User along with the other segment parameters.



SCM - TO - SIP DATA SEGMENT

FIGURE 2-10

Spare and Unused Fields - All spare and unused fields must be set to zero.

Command Control Field - This field identifies the segment as containing text following the BSL.

Precedence Field - The precedence parameter may be passed on to the user with the text. It indicates the urgency of the text.

TCP Version No. Field - The setting in this field is used to identify the proper user of SIP. If the TCP Version No. is invalid, the segment is discarded.

Source Subscriber Address Field - This field identifies the originating subscriber of this segment. This address may be passed on to the user as a parameter along with the text.

Destination Subscriber Address Field - This field should match this SIP's subscriber address. This address need not be passed on to the user as a parameter along with the text. If the address is invalid, the segment is discarded.

Security Fields - The two security fields settings must match and the security level must be within the maximum security authorization for this SIP's subscriber. If these tests (optional) hold, then the security level is passed on to the user as a parameter along with the text. If any of the above tests fail, the segment is discarded.

TCC Fields - The two TCC fields settings must match and the TCC designation must be authorized for this SIP's subscriber. If these tests (optional) hold, then the TCC code is passed on to the user as a parameter along with the text. If any of the above tests fail, the segment is discarded.

2.3.2 Ready for Next Segment (RFNS)

This command regulates the flow of segments from the SIP to the SCM. The command includes the parameter, W, which is the number of data segments that may be sent by the SIP to the SCM. This command will be sent by the SCM periodically. Presently the design calls for updating the window every second. The window is global, in the sense that it does not specify to what destination the segments must be sent. It does, however, represent the

general health of all the flows that the SIP is utilizing. A flow is a stream of segments of a single category to one particular destination. If several flows are congested either at source, tandem, or destination switches, they will tend to constrict the global window. The window will never recede to zero as long as some flows exist that are not congested. Category I flows will not normally be congested since these packets/segments are given highest processing priority at all switches. But if CAT I flows are congested (because of too many CAT I segments queued for output at the output SIP access line, for example) along with all other flows then the window will shrink to near zero (minimum window update is w=1). Therefore, a zero window restricts all data segments, CAT I and non-CAT I, from transmission to the SCM. The RFNS command is accepted and processed by SIP in all but INTERFACE DOWN states. The window in the RFNS command replaces the present value of the window. The window represents the new allocation. If SIP is in the W=0 state and this command is received, SIP moves to the READY state and dequeues and transmits to the SCM any held segments.

The proper format of the received RFNS segment is explained below and depicted in Figure 2-11.

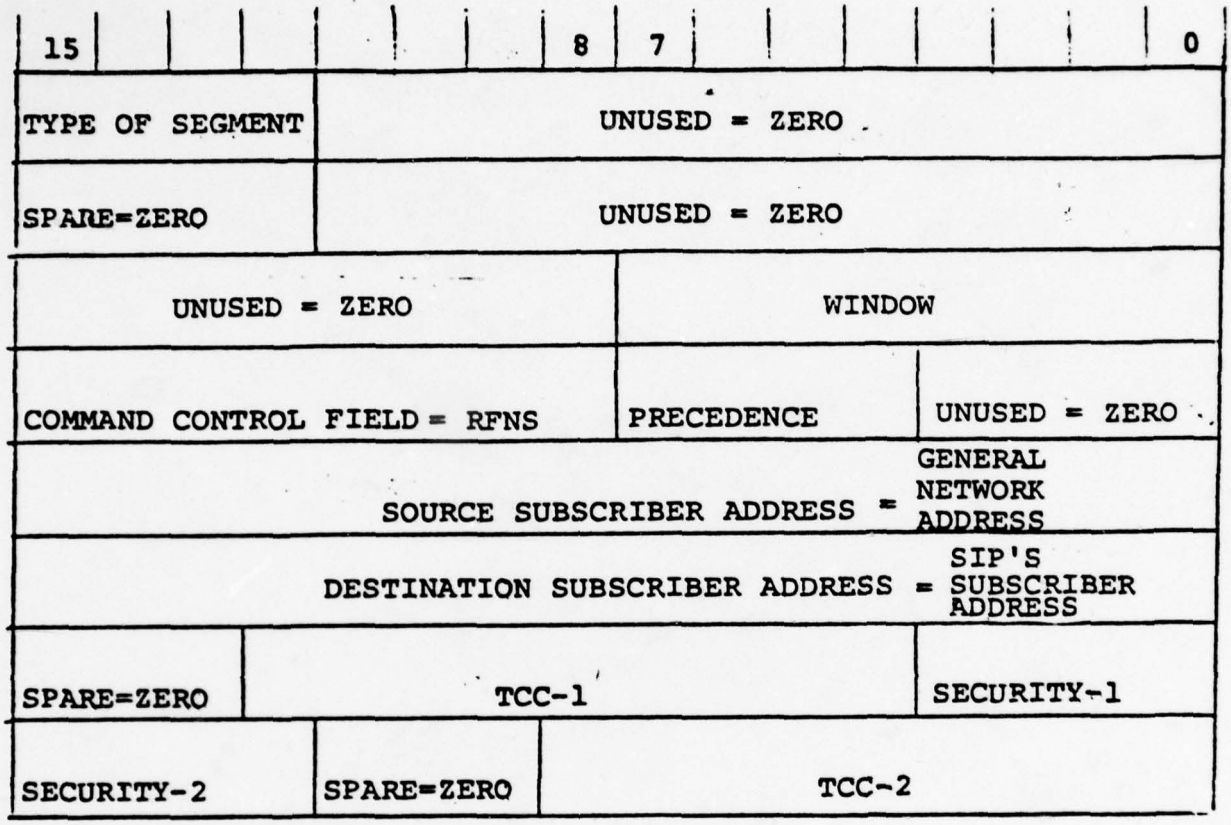
Type of Segment Field - This field is ignored.

Unused and Spare Fields - All unused and spare fields must be set to zero.

Window Field - This field will contain the number of data segments that the SIP can send to the SCM. This window replaces any previous window.

Command Control Field - This field will identify the segment as a Ready for Next Segment command.

Precedence Field - This field will contain the precedence level of the segment.



SCM - TO - SIP RFNS SEGMENT

FIGURE 2-11

Source Subscriber Address Field - This field will contain the general network address.

Destination Subscriber Address Field - This field will contain this SIP's subscriber address.

Security Fields - The two security fields must match and be any authorized security level for SCM-to-SIP exit line. If the test (optional) fails, the segment is discarded.

TCC Fields - The two TCC fields must match and the value must be an authorized TCC code fot this SIP's subscriber. If the test (optional) fails, then the segment is discarded.

2.3.3 Validation Reject, Error Reject, and Non-Delivery Notice

These notices indicate that the backbone has discarded the specified segment. The Non-Delivery Notice (NDN) indicates that the segment specified was discarded because of one of the following reasons:

- Destination Subscriber is Down
- Destination Subscriber Circuit is Down
- Destination Subscriber is Busy
- Traffic Acceptance Category Too Low
- Rejected, beyond Global Window
- Congestion at the Source SCM
- Congestion at a Backbone Trunk
- Congestion at the Destination Access Line
- Network Discard

The Validation Reject identifies the following causes:

- Invalid security - indicates that the security fields within the segment leader were inconsistent with each other, did not contain valid security information for the source or destination access circuit, or contained an unknown security code.
- Invalid TCC - indicates that an SCM has determined that the TCC fields of the segment leader are inconsistent with each other or invalid for the source or destination access circuit.

- o Invalid address - indicates that the segment leader destination address is unknown to the validating SCM.
- o Invalid precedence - indicates that the segment precedence field value exceeds the authorized precedence level for source access line.

The Error Reject command indicates that the source SIP has transmitted a segment with an invalid leader or that the leader was garbled within the validating SCM. If the Segment I.D. is ungarbled the user may be able to identify the segment and retransmit it.

These notices are accepted by SIP in all states except in the INTERFACE DOWN state. These notices are passed on to the User along with the discarded segments's original parameters. The original segment I.D. is passed on, since this will uniquely identify the particular segment and enable the User to recover if possible. The BSL of the discarded segment is returned unmodified except the appropriate cause placed on the Command Control Field and the source and destination address fields switched.

The proper format of the received segments is explained below and depicted in Figure 2-12.

Type of Segment Field - This field is ignored.

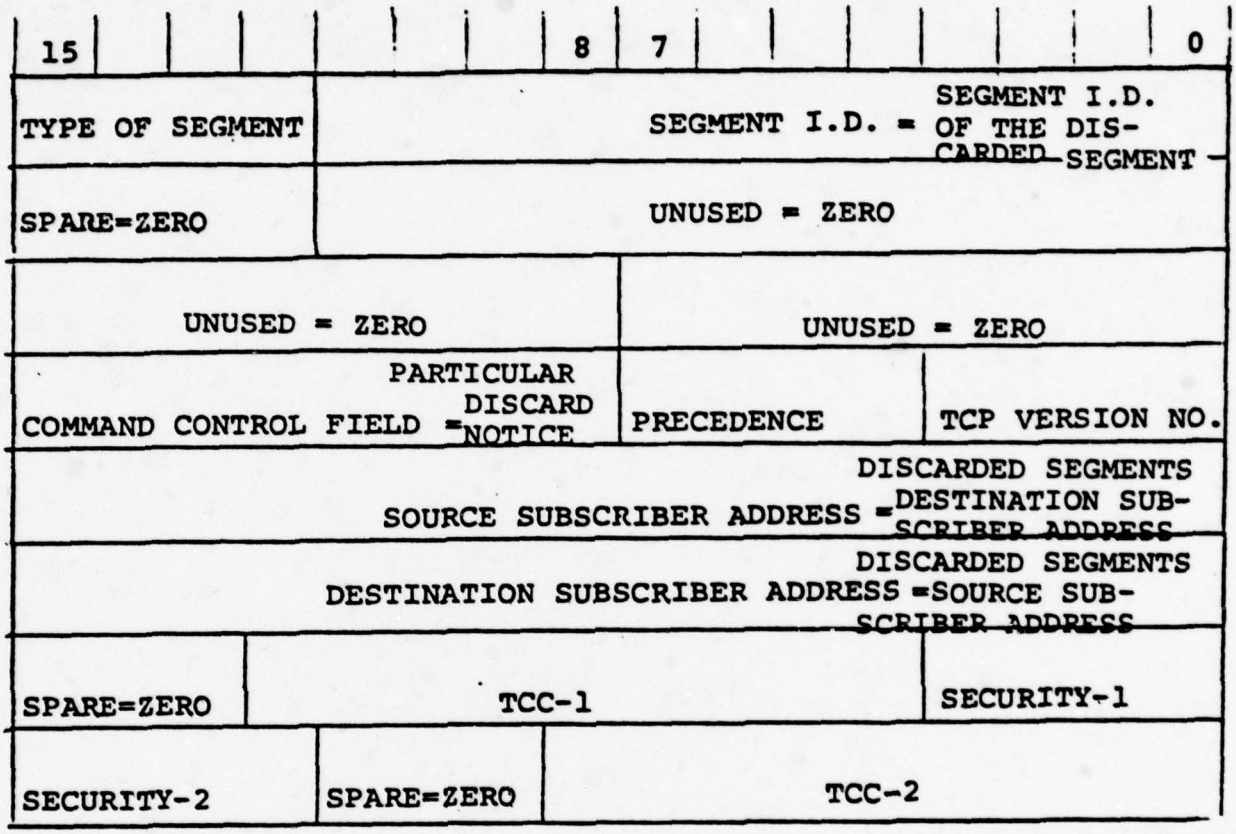
Segment I.D. Field - The original segment's segment I.D. is in this field. This field is passed on to the User as a parameter.

Spare and Unused Fields- All of these fields should be set to zero.

Command Control Field - This field identifies the particular discard notice. This cause may be passed on to the User.

Precedence Field - The precedence of the original segment is contained in this field and may be passed on to the User. The precedence value is not validated by SIP.

TCP Version No. Field - This field will identify the User who originated the original segment.



VALIDATION REJECT, ERROR REJECT, AND NON-DELIVERY, NOTICE SEGMENTS

FIGURE 2-12

Source Subscriber Address Field - This field contains the discarded segment's destination subscriber address and may be passed on to the User.

Destination Subscriber Address Field - This field contains the discarded segment's source subscriber address. This should match with the SIP's subscriber address, otherwise the segment is discarded.

Security Fields - These fields contain the original segment's security level. The parameter may be passed on to the User. The two security fields should not be validated.

TCC Fields - These fields contain the original segment's TCC code. It may be passed on to the User. The two TCC fields should not be validated.

2.3.4 SCM Status

This command indicates the status of the SCM and the access line between the SCM and SIP. Five subcommands have been defined to allow identification of SCM going down, SCM operable, access circuit going inoperable, access circuit operable, and SCM Busy.

Parameters associated with the SCM going-down subcommand will indicate how soon (Start Time), the reason (Reason for Outage) and the expected duration. Start Time specifies how soon the SCM will be going down in number of minutes from current time; Duration specifies when the SCM expects to again become operable in minutes from start time; and the RFO contains a reason code. Currently identified reason codes are scheduled maintenance, detected hardware/software failure, and switchover.

The SCM operable subcommand is issued when the SCM actually becomes operational after initialization, or after the SCM has recovered from an inoperable state as previously described. The Access-Circuit-Operable subcommand indicates that the access

circuit is operating. The access circuit includes transmission media, crypto, and modems.

The Access-Circuit-Going-Inoperable subcommand indicates that the access circuit is going inoperable. Parameters associated with this subcommand will indicate how soon (Start Time), the reason (Reason For Outage) and the expected duration (Duration). Start Time is the time in minutes from the current time, RFO contains a reason code and Duration indicates when the access line will again become operable.

The SCM Busy subcommand indicates that the SCM is temporarily unable to handle any more segments from the SIP, and moves SIP to the SCM RNR state from all states except SIP RNR and INTERFACE DOWN. From these states SIP moves to the INTERFACE DOWN state.

The inoperable subcommands on reception by the SIP will transition it to the INTERFACE DOWN state at the indicated time from all states. In this state no data segments can traverse the SIP/SCM link. The operable subcommands are explicit indications that the SCM or access line is backup. These notices along with the Mode VI initialization indication transition SIP to W=0 state where he waits for a window update from the SCM. The Operable subcommands are also used to negate an SCM Busy subcommand. The SCM Status notice may be delivered to the User such that he can flow control and notify his sources.

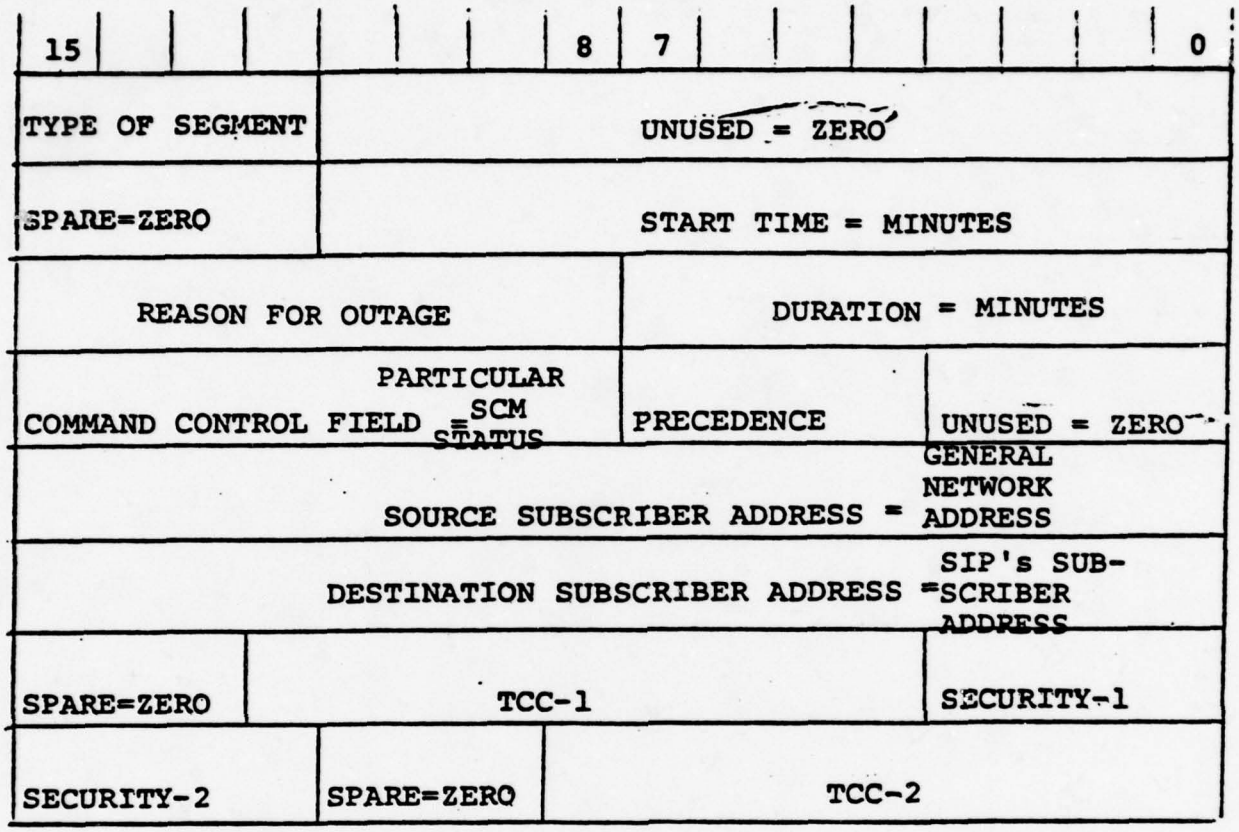
The proper format of the received segment is explained below and depicted in Figure 2-13.

Type of Segment Field - This field is ignored.

Unused and Spare Fields - All unused and spare fields should be set to zero.

Start Time Field - This field is unused except for SCM going inoperable and Access Line going inoperable. For these commands the start time field will contain the number minutes (binary number) from the current time that the down condition will begin.

Duration Field - This field remains unused except for the Inoperable subcommands. When it exists, it indicates the duration of the down condition in minutes (binary number).



SCM - TO - SIP SCM STATUS SEGMENT

FIGURE 2-13

Reason Field - This field will contain the cause for impending down condition. The codes are listed in Figure 2-14.

Command Field - This field will indicate the SCM Status subcommand.

Precedence Field - This field will contain the precedence level of the segment.

Source Subscriber Address Field - This field will contain the general network address.

Destination Subscriber Address Field - This field will contain the receiving SIP address. If this address does not match the SIP's subscriber address, the segment is discarded.

Security Fields - The two security fields must match and be any security level assigned to the SIP's subscriber.

TCC Fields - The two TCC codes must match and any authorized TCC code assigned to the SIP's subscriber is acceptable.

2.3.5 Echo

The Echo Request subcommand requests that the SIP Echo reply the entire segment. Echo Requests are accepted only in the READY state. In all other states, the segment is discarded. When accepted an Echo Reply is sent as described in paragraph 2.2.4. Echo Replies are validated and processed like any other data segment.

The proper format of the received Echo Request segment is explained below and depicted in Figure 2-15.

Type of Segment Field - This field is ignored but unchanged when responding to an Echo Request.

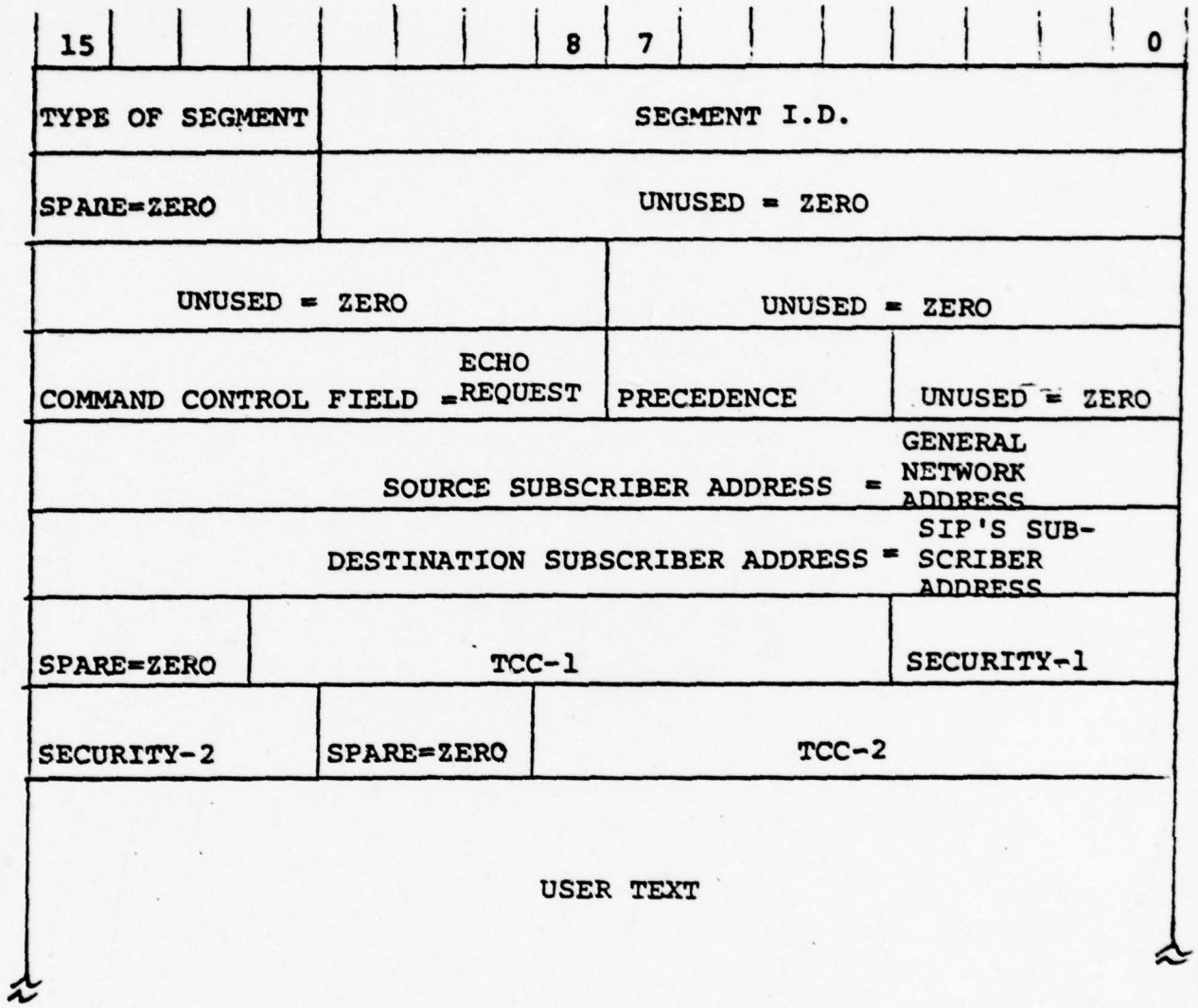
Segment I.D. Field - This field can be used by the SCM to identify the Echo segment. It is left unchanged when responding with Echo Reply.

Unused and Spare Fields - All unused and spare fields should be zero.

15 CODE 8	REASON
00000000	SCHEDULED MAINTENANCE
00000001	DETECTED HARDWARE SOFTWARE FAILURE
00000010	SWITCHOVER

SCM STATUS REASON FOR OUTAGE CODES

FIGURE 2-14



SCM - TO - SIP ECHO REQUEST SEGMENT

FIGURE 2-15

Command Control Field - This field identifies the segment as an Echo Request segment.

Precedence Field - This field may be set to any authorized precedence level of the SIP.

Source Subscriber Address Field - This field is set to the general network address.

Destination Subscriber Address Field - This field contains this SIP's subscriber address field.

Security Fields - These fields must match and contain an authorized security level for this SIP's subscriber.

TCC Fields - These fields must match and contain an authorized TCC code for this SIP's subscriber.

The proper format of the received echo reply segment is explained below and depicted in Figure 2-16.

Type of Segment Field - This field is ignored.

Segment I.D. Field - This field identifies the echo segment to the User.

Unused and Spare Fields - All unused and spare fields are zero.

Command Control Field - This field indicates that the segment is a data segment.

Precedence Field - The precedence assigned to the echo segment by the User is returned in the echo reply.

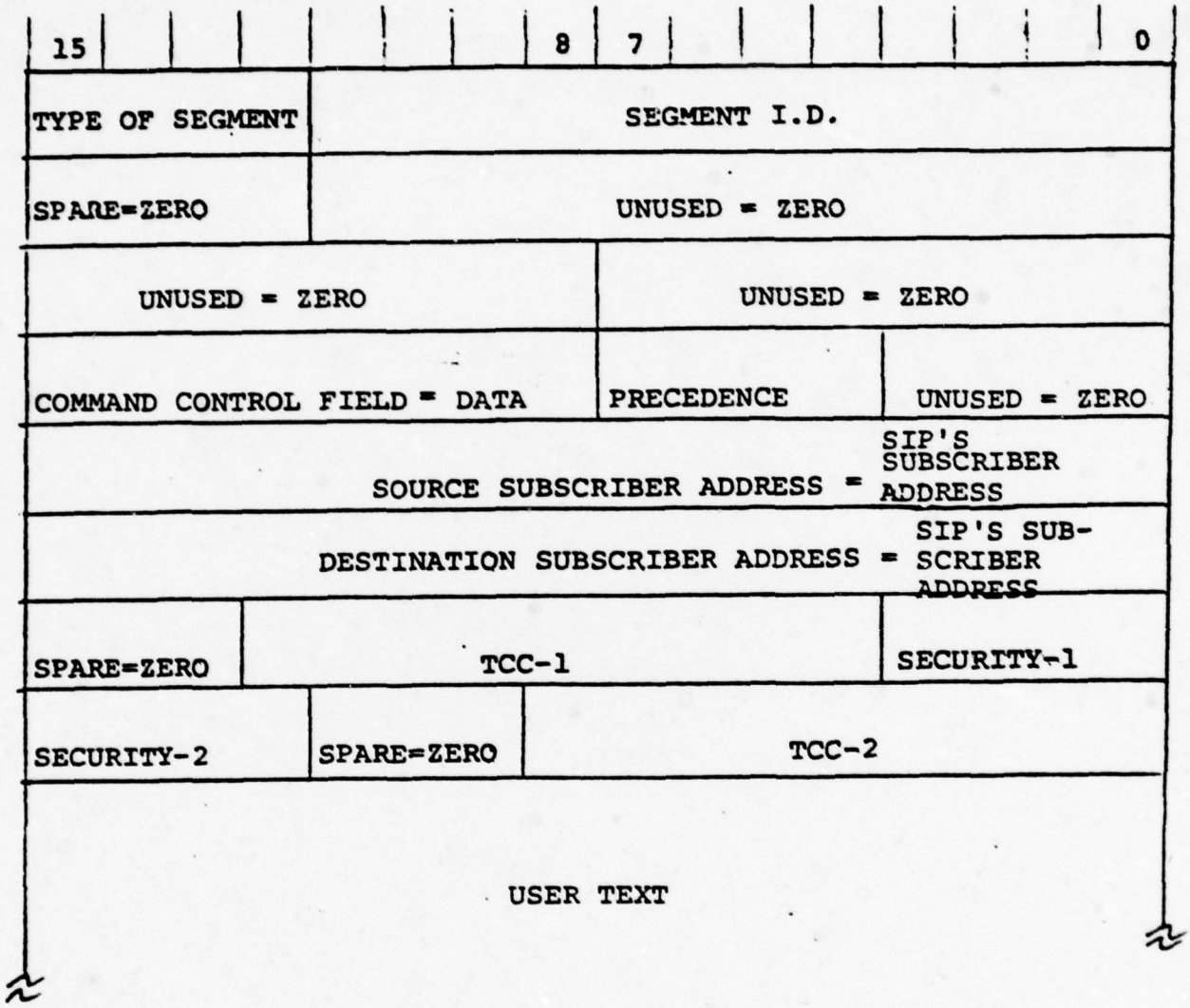
Source Subscriber Address Field - This field contains the SIP's subscriber address.

Destination Subscriber Address Field - This field contains SIP's subscriber address.

Security Fields - The security fields must match and be a level authorized for this SIP's User. These fields may be checked and passed on to the User.

TCC Fields - The TCC fields must match and the TCC must be an authorized code for this SIP's User.

Text Fields - Any text portions are returned to the User along with the above parameters.



SCM-TO-SIP ECHO REPLY
SEGMENT

FIGURE 2-16

SECTION 3

STATE/STIMULUS DESCRIPTION

A complete state description of SIP is contained in this section in the form of state transition charts. For each state of the five states a State Chart is present. Five states are identified:

READY

W=O

SIP RNR

SCM RNR

INTERFACE DOWN

Under the column Stimulus are listed the entire set of stimuli. The stimuli are broken out as follows:

User Stimuli

- User segment
- Subscriber Going Inoperable
- Subscriber Access Circuit Going Inoperable
- Subscriber Operable
- Subscriber Busy
- Echo Request

Network Stimuli

- Data
- Echo Request
- Ready For Next Segment
- SCM Going Inoperable
- SCM Busy
- SCM Operable
- Access Line Going Inoperable
- Access Line Operable
- Validation Reject
- Error Reject
- Non-Delivery Notice

Mode VI Stimuli

- Mode VI RNR
- Mode VI Initialized

Internal Stimuli

- Request Window Timeout
- Zero Window
- Initialization
- Request Window Threshold

When a stimulus is applied to a SIP state, SIP will either transition to another state or stay in the same state. The next state SIP moves to is listed under the column Next State. Any outputs that result from the state transition are listed under the columns User, Internal, Mode VI and Network. Outputs to the user consist of data segments and status messages. Outputs to the internal mechanisms consist of setting timers, discarding segments and queueing and dequeueing held segments. Outputs to Mode VI are segments, initialization and set Mode VI RNR. Finally, outputs to the network consist of data segments and status and control messages.

SIP STATE = READY

	Stimulus	Next State	OUTPUT			
From	Type		User	Internal	Mode VI	Network
USER	User Segment	Ready		Decrement W	Segment	Data Segment
	Subscriber Going Inoperable	Ready(Interface Down at time indicated)			Segment (RNR Mode VI at time indicated)	Subscriber Going Inoperable
	Subscriber Access Circuit Going Inoperable	Ready(Interface Down at time indicated)			Segment (RNR Mode VI at time indicated)	Subscriber Access Circuit Going Inoperable
	Subscriber Operable	Ready	SCM Operable		Segment	Subscriber Operable
	Subscriber Busy	SIP RNR			Segment	Subscriber Busy
	Echo Request	Ready		Decrement W	Segment	Self-Addressed Data Segment
NETWORK	Data from Net.	Ready	User Segment			
	Echo Request	Ready			Segment	Echo. Reply

SIP STATE = READY (Cont'd)

From	Stimulus Type	Next State	OUTPUT User	Internal	Mode VI	Network
	Ready for Next Segment	Ready		Update window		
	SCM Going Inoperable	Ready(Interface Down at time indicated)	SCM Going Inoperable		(RNR Mode VI at time indicated)	
	SCM Busy	SCM RNR	SCM Busy			
	SCM Operable	Ready	SCM Operable			
NETWORK	Access Line Going Inoperable	Ready(Interface Down at time indicated)	Access Line Going Inoperable		(RNR Mode VI at time indicated)	
	Access Line Operable	Ready	Access Line Operable			
	Validation Reject	Ready	Segment Reject with cause			
	Error Reject	Ready	Segment Reject with cause			
	Non Delivery Notice	Ready	Segment Reject with cause			

	Stimulus	Next State	OUTPUT			
From	Type		User	Internal	Mode VI	Network
MODE VI	Mode VI RNR	Interface Down	Access Line Inoperable			
	Mode VI Initialized	W=0	Access Line Operable	Set Timer	Segment	Subscriber Operable
INTERNAL	Request Window Threshold	Ready		Ignore		
	Request Window Timeout	Ready		Ignore		
	Zero Window	W=0		Set Timer		
	Initialization	Interface Down			Initialize Mode VI	

SIP STATE = W=O

	Stimulus	Next State	OUTPUT			
From	Type		User	Internal	Mode VI	Network
USER	User Segment	W=O		Hold Queue		
	Subscriber Going Inoperable	W=O (Interface Down at time indicated)			Segment (RNR Mode VI at time indicated)	Subscriber Going Inoperable
	Subscriber Access Circuit Going Inoperable	W=O (Interface Down at time indicated)			Segment (RNR Mode VI at time indicated)	Subscriber Access Circuit Going Inoperable
	Subscriber Operable	W=O			Segment	Subscriber Operable
	Subscriber Busy	SIP RNR			Segment	Subscriber Busy
	Echo Request	W=O		Hold Queue		
NETWORK	Data from Net.	W=O	User Segment			
	Echo Request	W=O			Segment	Echo Reply

	Stimulus	Next State	OUTPUT			
From	Type		User	Internal	Mode VI	Network
	Ready for Next Segment	Ready		Update Window, Dequeue Held Segments, Decrement W	Segments	Data Segments
	SCM Going Inoperable	W=0(Interface Down at time indicated)	SCM Going Inoperable		(RNR Mode VI at time indicated)	
	SCM Busy	SCM RNR	SCM Busy-Return Held Segments	Dequeue Held Segments		
	SCM Operable	W=0	SCM Operable			
N E T W O R K	Access Line Going Inoperable	W=0(Interface Down at time indicated)	Access Line Going Inoperable		(RNR Mode VI at time indicated)	
	Access Line Operable	W=0	Access Line Operable			
	Validation Reject	W=0	Segment Reject with cause			
	Error Reject	W=0	Segment Reject with cause			
	Non Delivery Notice	W=0	Segment Reject with cause			

SIP STATE = W=O (Cont'd)

	Stimulus	Next State	OUTPUT			
From	Type		User	Internal	Mode VI	Network
MODE VI	Mode VI RNR	Interface Down	Access Line Inoperable			
	Mode VI Initialized	W=O		Set timer	Segment	Subscriber Operable
INTERNAL	Request Window Threshold	SCM RNR	SCM Busy Return Held Segments	Dequeue Held Segments		
	Request Window Timeout	W=O			Segment	Request Window
	Zero Window	W=O		Ignore		
	Initialization	Interface Down			Initialize Mode VI	

SIP STATE = SIP RNR

	Stimulus	Next State	OUTPUT			
From	Type		User	Internal	Mode VI	Network
USER	User Segment	SIP RNR		Held if window is zero, otherwise decrement W	Segment	Data Segment if window is not zero
	Subscriber Going Inoperable	SIP RNR (Interface Down at time indicated)			Segment (RNR Mode VI at time indicated)	Subscriber Going Inoperable
	Subscriber Access Circuit Going Inoperable	SIP RNR (Interface Down at time indicated)			Segment (RNR Mode VI at time indicated)	Subscriber Access Circuit Going Inoperable
	Subscriber Operable	W=0, if window is zero - Ready, if window is non zero		Set Timer if window is zero	Segment	Subscriber Operable
	Subscriber Busy	SIP RNR			Segment	Subscriber Busy
	Echo Request	SIP RNR		Discard		
NETWORK	Data from Net.	SIP RNR		Discard	Segment	Subscriber Busy
	Echo Request	SIP RNR		Discard	Segment	Subscriber Busy

SIP STATE = SIP RNR (Cont'd)

	Stimulus	Next State	OUTPUT			
From	Type		User	Internal	Mode VI	Network
	Ready for Next Segment	SIP RNR		Update window Dequeue held segment, decrement W	Segment	Data-segment
	SCM Going Inoperable	SIP RNR(Interface Down at time indicated)	SCM Going Inoperable		(RNR Mode VI at time indicated)	
	SCM Busy	Interface Down	SCM Busy		RNR Mode VI	
	SCM Operable	SIP RNR	SCM Operable			
N E T W O R K	Access Line Going Inoperable	SIP RNR(Interface Down at time indicated)	Access Line Going Inoperable		(RNR Mode VI at time indicated)	
	Access Line Operable	SIP RNR	Access Line Operable			
	Validation Reject	SIP RNR	Segment Reject with cause			
	Error Reject	SIP RNR	Segment Reject with cause			
	Non Delivery Notice	SIP RNR	Segment Reject with cause			

SIP STATE = SIP RNR (Cont'd)

	Stimulus	Next State	OUTPUT			
From	Type		User	Internal	Mode VI	Network
MODE VI	Mode VI RNR	Interface Down	Access Line Inoperable			
	Mode VI Initialized	SIP RNR	Access Line Operable	Set Timer	Segment	Subscriber Busy
INTERNAL	Request Window Threshold	Interface Down	SCM Busy Return Held Segments	Dequeue Held Segments (Ignore if window not zero)	RNR Mode VI	
	Request Window Timeout	SIP RNR		Ignore if window not zero	Segment if window is zero	Request Window if zero Window
	Zero Window	SIP RNR		Set Timer		
	Initialization	Interface Down			Initialize Mode VI	

SIP STATE = SCM RNR

	Stimulus	Next State	OUTPUT			
From	Type		User	Internal	Mode VI	Network
USER	User Segment	SCM RNR	SCM Busy Return Segment			
	Subscriber Going Inoperable	SCM RNR (Interface Down at time indicated)			(RNR Mode VI at time ind.)	
	Subscriber Access Circuit Going Inoperable	SCM RNR (Interface Down at time indicated)			(RNR Mode VI at time ind.)	
	Subscriber Operable	SCM RNR	SCM Busy			
	Subscriber Busy	Interface Down			(RNR Mode VI)	
	Echo Request	SCM RNR	SCM Busy	Discard		
NETWORK	Data from Net.	SCM RNR	User Segment			
	Echo Request	SCM RNR		Discard		

SIP STATE = SCM RNR (Cont'd)

	Stimulus	Next State	OUTPUT			
From	Type		User	Internal	Mode VI	Network
	Ready for Next Segment	Ready	SCM Operable	Update Window		
	SCM Going Inoperable	SCM RNR (Interface Down at time indicated)	SCM Going Inoperable		(RNR Mode VI at time indicated)	
	SCM Busy	SCM RNR	SCM Busy			
	SCM Operable	W=0	SCM Operable	Set Timer		
N E T W O R K	Access Line Going Inoperable	SCM RNR (Interface Down at time ind.)	Access Line Going Inoperable		(RNR Mode VI at time indicated)	
	Access Line Operable	W=0	Access Line Operable	Set Timer		
	Validation Reject	SCM RNR	Segment Reject with cause			
	Error Reject	SCM RNR	Segment Reject with cause			
	Non Delivery Notice	SCM RNR	Segment Reject with cause			

SIP STATE = SCM RNR (Cont'd)

	Stimulus	Next State	OUTPUT			
From	Type		User	Internal	Mode VI	Network
MODE VI	Mode VI RNR	Interface Down	Access Line Inoperable			
	Mode VI Initialized	SCM RNR		Ignore		
INTERNAL	Request Window Threshold	SCM RNR		Ignore		
	Request Window Timeout	SCM RNR		Ignore		
	Zero Window	SCM RNR		Ignore		
	Initialization	Interface Down			Initialize Mode VI	

SIP STATE = INTERFACE DOWN

	Stimulus	Next State	OUTPUT			
From	Type		User	Internal	Mode VI	Network
USER	User Segment	Interface Down	Access Line Inoperable Return Segment			
	Subscriber Going Inoperable	Interface Down		Ignore		
	Subscriber Access Circuit Going Inoperable	Interface Down		Ignore		
	Subscriber Operable	W=O		Set Timer	Initialize Mode VI	
	Subscriber Busy	Interface Down		Ignore		
	Echo Request	Interface Down	Access Line Inoperable	Discard		
NETWORK	Data from Net.	Interface Down		Discard		
	Echo Request	Interface Down		Discard		

SIP STATE = INTERFACE DOWN (Cont'd)

	Stimulus	Next State	OUTPUT			
From	Type		User	Internal	Mode VI	Network
NETWORK	Ready for Next Segment	Interface Down		Discard		
	SCM Going Inoperable	Interface Down		Discard		
	SCM Busy	Interface Down		Discard		
	SCM Operable	Interface Down		Discard		
	Access Line Going Inoperable	Interface Down		Discard		
	Access Line Operable	Interface Down		Discard		
	Validation Reject	Interface Down		Discard		
	Error Reject	Interface Down		Discard		
	Non Delivery Notice	Interface Down		Discard		

SIP STATE = INTERFACE DOWN (Cont'd)

	Stimulus	Next State	OUTPUT			
From	Type		User	Internal	Mode VI	Network
MODE VI	Mode VI RNR	Interface Down		Ignore		
	Mode VI Initialized	W=0		Set Timer	Segment	Subscriber Operable
INTERNAL	Request Window Threshold	Interface Down		Ignore		
	Request Window Timeout	Interface Down		Ignore		
	Zero Window	Interface Down		Ignore		
	Initialization	Interface Down			Initialize Mode VI	